ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Combinatorial Theory, Series A 106 (2004) 123–143

Journal of Combinatorial Theory Series A

http://www.elsevier.com/locate/jcta

Quasirandom permutations

Joshua N. Cooper

Department of Mathematics, University of California, San Diego, La Jolla, California, USA

Received 6 October 2003

Abstract

Chung and Graham (J. Combin. Theory Ser. A 61 (1992) 64) define quasirandom subsets of $\mathbb{Z}_n$ to be those with any one of a large collection of equivalent random-like properties. We weaken their definition and call a subset of $\mathbb{Z}_n$ ε-balanced if its discrepancy on each interval is bounded by εn. A quasirandom permutation, then, is one which maps each interval to a highly balanced set. In the spirit of previous studies of quasirandomness, we exhibit several random-like properties which are equivalent to this one, including the property of containing (approximately) the expected number of subsequences of each order-type. We present a construction for a family of strongly quasirandom permutations, and prove that this construction is essentially optimal, using a result of Schmidt on the discrepancy of sequences of real numbers.

Keywords: Quasirandomness; Discrepancy; Permutations

1. Introduction

In recent years, combinatorialists have been investigating several realms of random-like—"quasirandom"—objects. For a given probability space $\mathscr{X}$, the basic idea is to choose some collection of properties that large objects in $\mathscr{X}$ have almost surely, and define a sequence $\{X_i\}_{i=1}^{\infty} \subset \mathscr{X}$ to be *quasirandom* if X_i has these properties in the limit. Often, this approach amounts to choosing some random variables η_j defined on $\mathscr{X}$ which tend to their expected values almost surely as $|X| \to \infty$, and defining X_i to be quasirandom when $(\eta_0(X_i), \eta_1(X_i), \ldots) \to (\mathbb{E}\eta_0, \mathbb{E}\eta_1, \ldots)$ sufficiently quickly. The resulting definitions are explored by finding many such collections of properties and showing that quasirandomness with respect to any one of them is

E-mail address: cooper@cims.nyu.edu.

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2004.01.006

equivalent to all the rest—often rather surprisingly, since the properties may appear completely unrelated to one another. Quasirandom graphs, hypergraphs, set systems, subsets of $\mathbb{Z}_n$, and tournaments have all been examined in this way [4–6]. Quasirandom families of permutations have been defined in [12], and Gowers [9] has used a careful quantitative analysis of strongly quasirandom (''α-uniform'', in his terminology) subsets of $\mathbb{Z}_n$ as an integral component of his remarkable new proof of Szemerédi's Theorem. Quasirandom objects also have applications in algorithms as deterministic substitutes for randomly generated objects, in addition to their purely theoretical uses. In fact, specific types of random-like permutations have been used already in a number of contexts. Lagarias [11] constructed random-like permutations of a d-dimensional array of cells in order to solve a practical memory-mapping problem, and Alon [1] used ''pseudo-random'' permutations to improve on the best known deterministic maximum-flow algorithm of Goldberg and Tarjan. Quasirandom sequences of reals are also fundamental to the extensively studied ''quasi-Monte Carlo'' methods of numerical analysis [13]. In this paper, we add (individual) permutations to the growing list of objects for which a formal notion of quasirandomness has been defined.

In Section 2, we discuss the concept of ε-balance, which weakens the quasirandomness of Chung and Graham. It is shown to be equivalent to several ''types'' of quasirandomness for subsets of $\mathbb{Z}_n$, including an infinite family of eigenvalue bounds. In Section 3, quasirandom permutations are defined as those which map intervals to uniformly balanced sets, and we prove that this definition is equivalent to several other random-like conditions. Section 4 contains a construction for a family of strongly quasirandom permutations that generalize the classical van der Corput sequences. We show that this construction is essentially optimal, using a result of Schmidt on the discrepancy of sequences of real numbers. Finally, Section 5 concludes with some open problems and directions for future work.

2. Balanced sets

Throughout the following, we consider permutations, i.e., elements of S_n, as actions on $\mathbb{Z}_n$ as well as sequences of numbers $(\sigma(0), \sigma(1), \ldots, \sigma(n-1))$ (''one-line notation''). When an ordering on $\mathbb{Z}_n$ is used, we mean the one inherited from $[0, n-1] \subset \mathbb{Z}$. If f_i, $i = 1, 2$, is a function from a totally ordered set A to a totally ordered set B_i, we say that f_1 and f_2 are *isomorphic* (and write $f_1 \sim f_2$) if, for any $a_1, a_2 \in A$, $f_1(a_1) < f_1(a_2)$ iff $f_2(a_1) < f_2(a_2)$. Note that this definition still makes sense when f_1 and f_2 are defined on different sets A_1 and A_2, so long as $|A_1| = |A_2|$ is finite and we identify them via the unique order-isomorphism between them. Then, if $\sigma \in S_n$ and $\tau \in S_m$, $m \leqslant n$, we say that τ occurs in σ at the set $A = \{a_i\}_{i=1}^m \subset \mathbb{Z}_n$ whenever $\sigma|_A \sim \tau$. For each $A \subset \mathbb{Z}_n$ and permutation τ, we write $\mathbf{X}_A^\tau(\sigma)$ for the indicator random variable of the event that τ occurs in σ at A, and we write $\mathbf{X}^\tau(\sigma)$ for the random variable that counts the number of occurrences of τ in σ, i.e., $\mathbf{X}^\tau(\sigma) = \sum_A \mathbf{X}_A^\tau(\sigma)$ where A ranges over all subsets of $\mathbb{Z}_n$ of cardinality m.

For any subset $S \subset \mathbb{Z}_n$ (or $S \subset \mathbb{Z}$), there is a minimal representation of S as a union of intervals. We call these intervals the *components* of S and denote the number of them by $c(S)$. Also, we adopt the convention that the symbols for a set and the characteristic function of that set be the same, so, for example, $S(x) = 1$ if $x \in S$ and $S(x) = 0$ if $x \notin S$. Finally, for any function from $\mathbb{Z}_n$ to $\mathbb{C}$, we write $\tilde{f}(k)$ for the kth Fourier coefficient of f, defined by

$$\tilde{f}(k) = \sum_{x \in \mathbb{Z}_n} f(x) e^{-2\pi i k x/n}.$$

A well-known alternative definition of the Fourier coefficients of a set S is the spectrum of the circulant matrix M_S whose (i,j) entry is $S(i+j)$.

One would expect random permutations to "jumble" the elements on which it acts, i.e., there should be no correlation between proximity in $\mathbb{Z}_n$ and proximity in the image. We can measure proximity by means of intervals: the elements of a small interval are all "close" to one another. Thus, if we define an interval of $\mathbb{Z}_n$ to be the projection of any interval of $\mathbb{Z}$, a permutation $\sigma \in S_n$ will be called "quasirandom" if the intersection of any interval I with the image of any other interval J under σ has cardinality approximately $|I||J|/n$, i.e., no interval contains much more or less of the image of any other interval than one would expect if σ were chosen randomly.

Thus, for any two sets $S, T \subset \mathbb{Z}_n$ we define the *discrepancy* of S in T as

$$D_T(S) = \left| |S \cap T| - \frac{|S||T|}{n} \right|.$$

Note that we may apply this definition to multisets S and T, and that it is symmetric in its arguments. Before proceeding, we present a simple lemma to the effect that D is subadditive.

Lemma 2.1. *If $S = A \cup B$, A and B disjoint, then $D_S(T) \leqslant D_A(T) + D_B(T)$. If $T = C \cup D$, C and D disjoint, then $D_S(T) \leqslant D_S(C) + D_S(D)$. That is, D is subadditive in both of its arguments.*

Proof. By the triangle inequality, we have

$$\begin{aligned} D_T(S) &= \left| |S \cap T| - \frac{|S||T|}{n} \right| \\ &= \left| |A \cap T| + |B \cap T| - \frac{|A||T|}{n} - \frac{|B||T|}{n} \right| \\ &\leqslant |D_T(A)| + |D_T(B)|. \end{aligned}$$

The other statement follows by symmetry. □

Define $D(S)$ to be the maximum of $D_J(S)$, taken over all intervals $J \subset \mathbb{Z}_n$, and call a set $S \subset \mathbb{Z}_n$ *ε-balanced* if $D(S) < \varepsilon n$. We state, for contrast, the definition of quasirandomness for a set $S \subset \mathbb{Z}_n$, studied by Chung and Graham [5]. (Here, and throughout the rest of this paper, we notationally suppress the fact that we actually mean an infinite sequence of sets S_i and a sequence $n_i \to \infty$.) In fact, the authors

showed that several definitions were equivalent, including all of the following. Let $s = |S|$ and $t = |T|$, and denote the characteristic function of S by χ.

1. (*Weak translation*) For almost all $x \in \mathbb{Z}_n$, $|S \cap (S + x)| = s^2/n + o(n)$.
2. (*Strong translation*) For all $T \subset \mathbb{Z}_n$, and almost all $x \in \mathbb{Z}_n$, $|S \cap (T + x)| = st/n + o(n)$.
3. (*k-pattern*) For almost all $u_1, u_2, \ldots, u_k \in \mathbb{Z}_n$,

$$\sum_x \prod_{i=1}^{k} \chi(x + u_i) = s^k/n^{k-1} + o(n).$$

4. (*Exponential sum*) For all $j \neq 0$ in $\mathbb{Z}_n$, $\sum_x \chi(x) \exp(2\pi i j x/n) = o(n)$.

It is easy to see that a set which is quasirandom in these senses is also $o(1)$-balanced. Indeed, for each interval $J \subset \mathbb{Z}_n$, "Strong translation" implies that $D_{J+x}(S) < \varepsilon n$ for some x with $|x| \leqslant \varepsilon n$. Therefore, since $|J \triangle (J + x)| \leqslant 2\varepsilon n$, this implies that $D_J(S) < 3\varepsilon n$. On the other hand, the set $S = \{2x \mid 0 \leqslant x \leqslant n - 1\} \subset \mathbb{Z}_{2n}$ is, for any $\varepsilon > 0$ and sufficiently large n, ε-balanced. However, $S \cap (S + t)$ does not have cardinality approximately $|S|^2/n$ for almost all t, i.e., it violates "Weak translation". Therefore, ε-balance is strictly weaker than quasirandomness in the sense of [5].

We use the convention that when "little oh" notation is used, convergence in n alone is intended. (That is, the convergence is uniform in any other quantities involved.) The following is the main result of this section.

Theorem 2.2. *For $r \in \mathbb{Z}_n$, we define $|r|$ to be the absolute value of the unique representative of r from the interval $(-n/2, n/2]$. Then, for any sequence of subsets $S \subset \mathbb{Z}_n$ and choice of $\alpha > 0$, the following are equivalent*:

[B] (*Balance*) $D(S) = o(n)$.
[PB] (*Piecewise balance*) *For any subset $T \subset \mathbb{Z}_n$, $D_T(S) = o(nc(T))$, where $c(T)$ denotes the number of components T.*
[MB] (*Multiple balance*) *Let kS denote the multiset $\{ks | s \in S\}$. Then, for any $k \in \mathbb{Z}_n \backslash \{0\}$, $D(kS) = o(n|k|)$.*
[E($\frac{1}{2}$)] (*Eigenvalue bound $\frac{1}{2}$*) *For all nonzero $k \in \mathbb{Z}_n$, $\tilde{S}(k) = o(n|k|^{1/2})$.*
[E(α)] (*Eigenvalue bound α*) *For all nonzero $k \in \mathbb{Z}_n$, $\tilde{S}(k) = o(n|k|^{\alpha})$.*
[S] (*Sum*) $\sum_{r \neq 0} (|\tilde{S}(k)|/|k|)^2 = o(n^2)$.
[T] (*Translation*) *For any interval J,*

$$\sum_{k \in \mathbb{Z}_n} \left(|S \cap (J + k)| - \frac{|S||J|}{n} \right)^2 = o(n^3).$$

We will show that [B] $\Rightarrow$ [PB] $\Rightarrow$ [MB] $\Rightarrow$ [E($\frac{1}{2}$)] $\Rightarrow$ [E(α)] $\Rightarrow$ [S] $\Rightarrow$ [T] $\Rightarrow$ [B]. In each case, a statement involving some ε is shown to imply the next for some $f(\varepsilon)$,

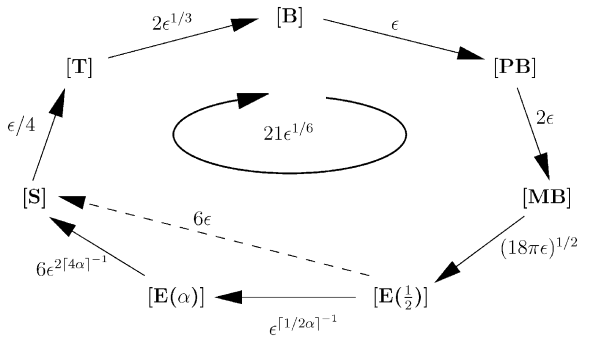

Fig. 1. Diagram of implications for Theorem 2.2.

where f is a function which tends to zero as its argument does. For example, Proposition 2.3 below states that if $D_T(S) < \varepsilon nc(T)$ for all T, then $D_T(kS) < 2\varepsilon n|k|$ for all k, so that $f(\varepsilon) = 2\varepsilon$. It appears to be theoretically useful to track what happens to ε as we pass through each implication—see, for example, [9]. Thus, we include Fig. 1 as an accompaniment to Theorem 2.2. (Note that, by the proof of Proposition 2.4, Fig. 1 is only valid for $\varepsilon < \pi/8$, though this is hardly a significant restriction.) The shortcut edge from [E($\frac{1}{2}$)] to [S] is given to illustrate the (best possible) choice of $\alpha = 1/4$ in [E(α)], and the circular arrow represents one complete traversal of the cycle of implications, including the shortcut edge.

Theorem 2.2 is proven in pieces, beginning with the following proposition.

Proposition 2.3. [B] $\Rightarrow$ [PB] $\Rightarrow$ [MB].

Proof. Suppose that $D(S) < \varepsilon n$. Then, by Lemma 2.1, for any T, $D_T(S) \leqslant \sum D_{T_i}(S)$, where the sum is over the components of T. Thus, $D_T(S) < \varepsilon n\, c(T)$, and [B] $\Rightarrow$ [PB].

Now, suppose [PB] holds for S. Note that, for a given $k \in \mathbb{Z}_n \backslash \{0\}$ and interval J, the set J' of elements $x \in \mathbb{Z}_n$ such that $kx \in J$ has at most $|k|$ components. Let J_i be the set of integer points (viewed as elements of $\mathbb{Z}_n$) lying in $[a/k, b/k] + in/k$, so that $J' = \bigcup_i J_i$. Then the cardinality of J_i is off from $|J|/k$ by at most 1. By [PB] and the triangle inequality,

$$\begin{aligned} D_J(kS) &= \left| |kS \cap J| - \frac{|S||J|}{n} \right| \\ &\leqslant \left| \sum_i |S \cap J_i| - \sum_i \frac{|S||J_i|}{n} \right| + \frac{|S|}{n} \left| \sum_i |J_i| - |J| \right| \\ &< \varepsilon n|k| + |k| \frac{|S|}{n} \leqslant 2\varepsilon n|k| \end{aligned}$$

since, trivially, $\varepsilon \geqslant n^{-1}$. $\square$

Now, we wish to show that multiple balance implies the first eigenvalue bound. The basic idea is to imbed the elements of S into the unit circle via the exponential

map, and then show that a great deal of cancellation happens because of the relatively uniform distribution of elements of S.

Proposition 2.4. [MB] $\Rightarrow$ [E($\frac{1}{2}$)].

Proof. Let $\omega = e^{2\pi i/n}$ and $J_m^j = [\frac{nj}{m}, \frac{n(j+1)}{m})$, and let ε be the bound on $(nk)^{-1}D(kS)$. Recall that $\varepsilon \geqslant n^{-1}$. First, we prove the following:

Claim. *Let m and j be positive integers with $0 \leqslant j < m$, and $m \geqslant 2$. If we define the multiset $S_j = kS \cap J_m^j$ and let $\gamma_j = \omega^{-n(j+1/2)/m}$, then*

$$\left| \sum_{x \in S_j} \omega^{-x} - \frac{|S|}{m}\gamma_j \right| < \frac{\pi|S|}{m^2} + 2\varepsilon|k|n.$$

Proof of Claim. We may write the left-hand side of the above expression as

$$\begin{aligned}
\left| \sum_{x \in S_j} \omega^{-x} - \frac{|S|}{m}\gamma_j \right| &= \left| \sum_{x \in S_j} \left(\omega^{-x} - \frac{|S|}{m|S_j|}\gamma_j \right) \right| \\
&\leqslant \frac{|S|}{m|S_j|} \left| \sum_{x \in S_j} (\omega^{-x} - \gamma_j) \right| + \left| \sum_{x \in S_j} \omega^{-x} \left(1 - \frac{|S|}{m|S_j|} \right) \right| \\
&\leqslant \frac{|S|}{m|S_j|} \sum_{x \in S_j} |(\omega^{-x} - \gamma_j)| + \sum_{x \in S_j} \left| \omega^{-x} \left(1 - \frac{|S|}{m|S_j|} \right) \right|.
\end{aligned}$$

Now, for $x \in S_j$,

$$|\omega^{-x} - \gamma_j| \leqslant |\omega^{-nj/m} - \omega^{-n(j+1/2)/m}| \leqslant \frac{n/2}{m} \cdot \frac{2\pi}{n} = \frac{\pi}{m}.$$

Plugging this expression in and applying [MB], we have

$$\begin{aligned}
\left| \sum_{x \in S_j} \omega^{-x} - \frac{|S|}{m}\gamma_j \right| &\leqslant \frac{|S|}{m|S_j|} \cdot |S_j| \cdot \frac{\pi}{m} + \left| |S_j| - \frac{|S|}{m} \right| \\
&\leqslant \frac{\pi|S|}{m^2} + \left| |kS \cap J_m^j| - \frac{|S||J_m^j|}{n} \right| + \frac{|S|}{n} \left| \frac{n}{m} - |J_m^j| \right| \\
&< \frac{\pi|S|}{m^2} + \varepsilon|k|n + \frac{|S|}{n} \\
&\leqslant \frac{\pi|S|}{m^2} + 2\varepsilon|k|n,
\end{aligned}$$

thus, proving the claim. $\square$

If we sum over all $j \in [0, m-1)$,

$$\begin{aligned}\left|\sum_{x\in S}\omega^{-kx}\right| &= \left|\sum_{j=0}^{m-1}\sum_{x\in S_j}\omega^{-x}\right| \\ &\leqslant \left|\sum_{j=0}^{m-1}\frac{|S|}{m}\gamma_j\right| + \sum_{j=0}^{m-1}\left|\sum_{x\in S_j}\omega^{-x} - \frac{|S|}{m}\gamma_j\right| \\ &< 0 + \frac{\pi|S|}{m} + 2\varepsilon|k|nm\end{aligned}$$

if we assume that $m \geqslant 2$. Thus, letting $m = \left\lfloor \left(\frac{\pi|S|}{2\varepsilon|k|n}\right)^{1/2} \right\rfloor$, we have

$$\left|\sum_{x\in S}\omega^{-kx}\right| < \sqrt{18\pi\varepsilon n|k||S|} \leqslant n\sqrt{18\pi\varepsilon|k|}$$

unless $m < 2$, i.e., $\varepsilon > \frac{\pi}{8}$, which is eventually impossible, given [MB]. We may therefore conclude that $|\tilde{S}(k)| = o(n|k|^{1/2})$. □

Before we proceed with the next implication, the following lemma will be necessary. It implies, surprisingly, that [E(α)] is equivalent to [E(β)] for all α and β.

Lemma 2.5. [E(α)] *implies* [E(β)] *for any* $\alpha, \beta > 0$.

Proof. Let $M = \left\lceil \frac{\alpha}{\beta} \right\rceil$, and assume [E(α)]. Then

$$|\tilde{S}(k)|^M = \left|\sum_{t\in\mathbb{Z}_n} S(t)\omega^{-kt}\right|^M = \left|\sum_{t_1,\ldots,t_M}\left[\prod_{j=1}^{M} S(t_j)\right]\omega^{-k\sum_{i=1}^{M} t_i}\right|.$$

Letting $u = \sum_{i=2}^{M} t_i$, we have

$$\begin{aligned}|\tilde{S}(k)|^M &= \left|\sum_{t_2,\ldots,t_M}\left[\prod_{j=2}^{M} S(t_j)\right]\sum_{t_1} S(t_1)\omega^{-k(t_1+u)}\right| \\ &\leqslant \sum_{t_2,\ldots,t_M}\left[\prod_{j=2}^{M} S(t_j)\right]\left|\sum_{t_1} S(t_1)\omega^{-kt_1}\right| \\ &= \sum_{t_2,\ldots,t_M}\left[\prod_{j=2}^{M} S(t_j)\right]|\tilde{S}(k)| \\ &< \sum_{t_2,\ldots,t_M}\left[\prod_{j=2}^{M} S(t_j)\right]\varepsilon n|k|^{\alpha} \\ &= |S|^{M-1}\varepsilon n|k|^{\alpha} \leqslant \varepsilon n^M|k|^{\alpha}.\end{aligned}$$

Thus, taking the Mth root of both sides, we have

$$|\tilde{S}(k)| < \varepsilon^{1/M} n|k|^{\alpha/M} \leqslant \varepsilon^{\lceil \alpha/\beta \rceil^{-1}} n|k|^{\beta}. \qquad \square$$

The following corollary is actually what is needed for Theorem 2.2.

Corollary 2.6. $[\mathrm{E}(\frac{1}{2})] \Rightarrow [\mathrm{E}(\alpha)]$.

Note that, to proceed with the next proposition, $\alpha = 1/2$ would not quite be enough—we *have* to reduce it by a bit with Proposition 2.5.

Proposition 2.7. $[\mathrm{E}(\alpha)] \Rightarrow [\mathrm{S}]$.

Proof. By Proposition 2.5, we know that $|\tilde{S}(k)| < \varepsilon^{\lceil 4\alpha \rceil^{-1}} n|k|^{1/4}$ for all $k \neq 0$. Then

$$\sum_{r \neq 0} \left(\frac{|\tilde{S}(k)|}{|k|} \right)^2 < \sum_{k \neq 0} \left(\frac{\varepsilon^{\lceil 4\alpha \rceil^{-1}} n|k|^{1/4}}{|k|} \right)^2 \leqslant \varepsilon^{2\lceil 4\alpha \rceil^{-1}} n^2 \sum_{k \neq 0} |k|^{-3/2} < 6\varepsilon^{2\lceil 4\alpha \rceil^{-1}} n^2,$$

where we have used the approximation $|\zeta(s)| < (Re(s) - 1)^{-1} + 1$ for s with $Re(s) > 1$. $\square$

We now write a cyclic sum in terms of Fourier coefficients. A proof of the following standard lemma is included for the sake of completeness.

Lemma 2.8. *If J is an interval of $\mathbb{Z}_n$, then $\tilde{J}(k) \leqslant \frac{n}{2|k|}$.*

Proof. We may write the magnitude of the kth Fourier coefficient of $J = [a+1, a+M]$ as

$$|\tilde{J}(k)| = \left| \sum_x J(x)\omega^{-kx} \right| = \left| \sum_{x=a}^{b} \omega^{-kx} \right| = \left| \sum_{x=1}^{M} \omega^{-kx} \right|$$
$$= \frac{|\omega^{-kM} - 1|}{|\omega^{-k} - 1|} \leqslant \frac{2}{4|k|/n} = \frac{n}{2|k|}$$

since $|e^{i\theta} - 1| \geqslant \frac{2|\theta|}{\pi}$ for all θ. $\square$

Proposition 2.9. $[\mathrm{S}] \Rightarrow [\mathrm{T}]$.

Proof. Assume that $\sum_{k \neq 0} \left(\frac{|\tilde{S}(k)|}{|k|} \right)^2 < \varepsilon n^2$. We may write the "translation" sum as

$$\sum_{k \in \mathbb{Z}_n} \left(|S \cap (J+k)| - \frac{|S||J|}{n} \right)^2 = \sum_{k \in \mathbb{Z}_n} |S \cap (J+k)|^2 - \frac{|S|^2|J|^2}{n}. \qquad (1)$$

Recall that M_S is the $n \times n$ matrix whose (i,j) entry is $S(i+j)$. Letting $\mathbf{v}$ be the vector $(J(0), J(1), \ldots)$, we find that $M_S\mathbf{v}$ is the vector whose kth entry is $|I \cap (J+k)|$. Therefore, letting $\phi_k = (1, \omega^k, \omega^{2k}, \ldots)$ be the kth eigenvector of M_S,

$$\begin{aligned}\sum_{k\in\mathbb{Z}_n} |S\cap(J+k)|^2 = |M_S\mathbf{v}|^2 &= \left| M_S \sum_k \frac{\langle \mathbf{v}, \phi_k\rangle}{|\phi_k|^2}\phi_k \right|^2 \\ &= \sum_k \left| \tilde{S}(k)^2 \frac{\langle \mathbf{v}, \phi_k\rangle^2}{|\phi_k|^2} \right| \\ &= \sum_{k\neq 0} \left| \tilde{S}(k)\frac{\tilde{J}(-k)}{\sqrt{n}} \right|^2 + \frac{|S|^2|J|^2}{n}.\end{aligned}$$

Applying this equality, property [S], and Lemma 2.8 to Eq. (1),

$$\begin{aligned}\sum_{k\in\mathbb{Z}_n} \left(|S\cap(J+k)| - \frac{|S||J|}{n} \right)^2 = \sum_{k\neq 0} \left| \tilde{S}(k)\frac{\tilde{J}(-k)}{\sqrt{n}} \right|^2 &\leqslant \frac{n}{4} \sum_{k\neq 0} \left| \frac{\tilde{S}(k)}{|k|} \right|^2 \\ &< \varepsilon n^3/4. \qquad \square\end{aligned}$$

To complete the circle of implications and finish the proof of Theorem 2.2, we show that ε-balance is implied by the "translation" property.

Proposition 2.10. [T] $\Rightarrow$ [B].

Proof. Suppose that, for some interval $J \subset \mathbb{Z}_n$,

$$\left| |S\cap J| - \frac{|S||J|}{n} \right| \geqslant 2\varepsilon^{1/3} n.$$

Then we may conclude that

$$\left| |S\cap(J+k)| - \frac{|S||J|}{n} \right| \geqslant \varepsilon^{1/3} n,$$

whenever $|k| \leqslant \varepsilon^{1/3} n$. Since there are at least $\varepsilon^{1/3} n$ such k's,

$$\sum_k \left| |S\cap(J+k)| - \frac{|S||J|}{n} \right|^2 \geqslant \varepsilon^{1/3} n \cdot \varepsilon^{2/3} n^2 = \varepsilon n^3$$

contradicting [T]. $\square$

3. Quasirandom permutations

In this section, we discuss several equivalent formulations of quasirandom permutations. The central definition is, roughly, that a quasirandom permutation is one which sends each interval to a highly balanced set. Thus, we will write $D(\sigma)$ for $\max(D_J(\sigma(I)))$, where the maximum is taken over all intervals I and J, and a sequence of permutations σ_j will be called *quasirandom* if $D(\sigma_j) = o(n)$. The following is the main result of this section.

Theorem 3.1. *For any sequence of permutations $\sigma \in S_n$ and integer $m \geqslant 2$ with $n > m$, the following are equivalent*:

[UB] (*Uniform balance*) $D(\sigma) = o(n)$.

[SP] (*Separability*) *For any intervals $I, J, K, K' \subset \mathbb{Z}_n$,*

$$\left| \sum_{x \in K \cap \sigma^{-1}(K')} I(x)J(\sigma(x)) - \frac{1}{n} \sum_{x \in K, y \in K'} I(x)J(y) \right| = o(n).$$

[mS] (*m-Subsequences*) *For any permutation $\tau \in S_m$ and intervals $I, J \subset \mathbb{Z}_n$ with $|I| \geqslant n/2$ and $|J| \geqslant n/2$, we have $|I \cap \sigma^{-1}(J)| \geqslant n/4 + o(n)$ and*

$$\mathbf{X}^{\tau}(\sigma|_{I \cap \sigma^{-1}(J)}) = \frac{1}{m!} \binom{|\sigma(I) \cap J|}{m} + o(n^m).$$

[2S] (2-*Subsequences*) *For any intervals $I, J \subset \mathbb{Z}_n$ with $|I| \geqslant n/2$ and $|J| \geqslant n/2$, we have $|I \cap \sigma^{-1}(J)| \geqslant n/4 + o(n)$ and*

$$\mathbf{X}^{(01)}(\sigma|_{I \cap \sigma^{-1}(J)}) - \mathbf{X}^{(10)}(\sigma|_{I \cap \sigma^{-1}(J)}) = o(n^2).$$

It follows immediately that these conditions are also equivalent to each interpretation of the statement "For all intervals $J \subset \mathbb{Z}_n$, $\sigma(J)$ is ε-balanced" given by the equivalences of Theorem 2.2. Thus, we have a total of 10 equivalent quasirandom properties: seven arising as "uniformly convergent" versions of the properties in Theorem 2.2 and three new ones, which are included with uniform balance in Fig. 2.

Again, we prove the theorem piece by piece, keeping track of ε as we go. The next result states that, if uniform balance is obeyed, then the variable x and its image under σ are nearly independent.

Proposition 3.2. [UB] $\Leftrightarrow$ [SP].

Proof. [UB] holds iff, for all intervals $I, J, K, K' \subset \mathbb{Z}_n$,

$$\left| |\sigma(I \cap K) \cap (J \cap K')| - \frac{1}{n} |I \cap K||J \cap K'| \right| < \varepsilon n.$$

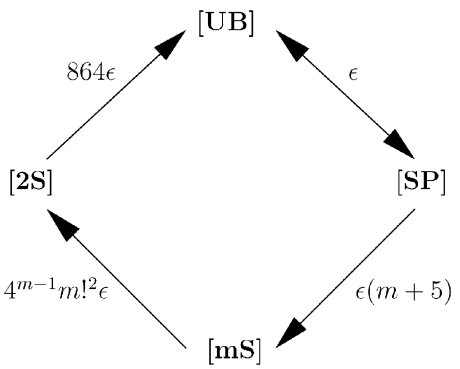

Fig. 2. Diagram of implications for Theorem 3.1.

But this quantity is equal to

$$\left| \sum_{x \in K \cap \sigma^{-1}(K')} I(x)J(\sigma(x)) - \frac{1}{n} \sum_{x \in K, y \in K'} I(x)J(y) \right|,$$

so that [UB] is equivalent to [SP]. □

Now, we show that the separability achieved in the last proposition is sufficient to imply that subsequences happen at the "right" rate (i.e., what one would expect of truly random permutations) on certain sets of indices. A simple lemma will aid in the proof.

Lemma 3.3. *If, for each j with $1 \leqslant j \leqslant k$, $|x_j - a_j| \leqslant \delta a_j \leqslant a_j$, then*

$$\left| \prod_{j=1}^{k} x_j - \prod_{j=1}^{k} a_j \right| < 2^k \delta \prod_{j=1}^{k} a_j.$$

We may now prove that [SP] $\Rightarrow$ [mS].

Proposition 3.4. [SP] $\Rightarrow$ [mS].

Proof. Let I, J be intervals with $|I| \geqslant n/2$ and $|J| \geqslant n/2$, and let $K = I \cap \sigma^{-1}(J)$. It is clear that [SP] implies that $|K| \geqslant n/4 + o(n)$. Note that we may write the number of "occurrences" of $\tau \in S_m$ in $\sigma|_K$ as

$$\mathbf{X}^{\tau}(\sigma|_K) = \sum_{x_1, \ldots, x_m \in K} \prod_{i=0}^{m} (\chi(x_i < x_{i+1}) \chi(\sigma(x_{\tau^{-1}(j)}) < \sigma(x_{\tau^{-1}(j+1)}))).$$

In the interest of notational compactness, we will denote $\chi(x<y)$ by $\langle x|y \rangle$, and define $\langle x|y \rangle = 1$ if either x or y is undefined. Furthermore, for any subset $A \subset [m]$,

we will denote the following expression

$$\sum_{\{x_i\}_{i\notin A}\subset K}\ \sum_{\{x_k\}_{k\in A}\subset I}\ \sum_{\{x'_k\}_{k\in A}\subset J}\left(\prod_{j=0}^{m}\langle x_j|x_{j+1}\rangle x^A_{\tau^{-1}(j)}|x^A_{\tau^{-1}(j+1)}\rangle\right)$$

by $\Sigma(A)$, where x_j^A means $\Sigma(x_j)$ for $j\notin A$, and x'_k for $j\in A$. Thus, $\mathbf{X}^\tau(\sigma|_K)=\Sigma(\emptyset)$. The proof will now proceed by induction on the subsets of $[m]$, ordered by inclusion.

Suppose $A\subset B\subset[m]$, with $B\backslash A=\{s\}$, and assume that

$$|\mathbf{X}^\tau(\sigma|_K)-n^{-|A|}\Sigma(A)|<|A|\varepsilon n^m. \tag{2}$$

By [SP], we know that, for any $a,b,c,d\in\mathbb{Z}_n$, the quantity

$$\left|\sum_{x_s\in K}\langle a|x_s\rangle\langle x_s|b\rangle\langle c|\sigma(x_s)\rangle\langle\sigma(x_s)|d\rangle - \frac{1}{n}\sum_{x_s\in I,x'_s\in J}\langle a|x_s\rangle\langle x_s|b\rangle\langle c|x'_s\rangle\langle x'_s|d\rangle\right|$$

is bounded above by εn. Then, substituting $a=x_{s-1}$, $b=x_{s+1}$, $c=x^A_{\tau^{-1}(\tau(s)-1)}$, and $d=x^A_{\tau^{-1}(\tau(s)+1)}$ to account for all the terms containing x_s in the product portion of the expression $\Sigma(A)$, we have (after a very messy but otherwise straightforward calculation),

$$|\Sigma(A)-n^{-1}\Sigma(B)|<\varepsilon n|K|^{m-|B|}|I|^{|A|}|J|^{|A|}\leqslant\varepsilon n^{m+|A|}.$$

Applying this to the inductive hypothesis with the aid of the triangle inequality yields

$$\begin{aligned}|\mathbf{X}^\tau(\sigma|_K)-n^{-|B|}\Sigma(B)|&\leqslant|\mathbf{X}^\tau(\sigma|_K)-n^{-|A|}\Sigma(A)|+n^{-|A|}|\Sigma(A)-n^{-1}\Sigma(B)|\\&<|A|\varepsilon n^m+n^{-|A|}\varepsilon n^{m+|A|}=|B|\varepsilon n^m.\end{aligned}$$

Therefore, (2) is true for all $A\subset[m]$. In particular, it is true for $A=[m]$, so that

$$|\mathbf{X}^\tau(\sigma|_K)-n^{-m}\Sigma([m])|<m\varepsilon n^m.$$

Since we have

$$\begin{aligned}\left|\sum_{\{x_j\}\subset I}\prod_{j=0}^{m}\langle x_j|x_{j+1}\rangle-\frac{|I|^m}{m!}\right|&=\left|\binom{|I|}{m}-\frac{|I|^m}{m!}\right|\leqslant\frac{(|I|+m)^m-|I|^m}{m!}\\&=\frac{1}{m!}\sum_{k=1}^{m}\binom{m}{k}|I|^{m-k}m^k\leqslant\frac{|I|^{m-1}}{m!}\sum_{k=0}^{m}\binom{m}{k}m^k\\&=\frac{(1+m)^m}{m!}|I|^{m-1}\end{aligned} \tag{3}$$

and also

$$\left|\sum_{\{x_j\}\subset J}\prod_{j=0}^{m}\langle x_j|x_{j+1}\rangle-\frac{|J|^m}{m!}\right|\leqslant\frac{(1+m)^m}{m!}|J|^{m-1},$$

we may conclude that

$$\left|\Sigma([m])-\frac{|I|^m|J|^m}{m!^2}\right|<4n^{2m-1}\frac{(1+m)^m}{m!^2}$$

by Lemma 3.3. Thus,

$$\begin{aligned}\left|\mathbf{X}^{\tau}(\sigma|_K)-\frac{1}{m!^2}\left(\frac{|I||J|}{n}\right)^m\right|&\leqslant\left|\mathbf{X}^{\tau}(\sigma|_K)-\frac{1}{n^m}\Sigma([m])\right|+\frac{1}{n^m}\left|\Sigma([m])-\frac{|I|^m|J|^m}{m!^2}\right|\\&<m\varepsilon n^m+4n^{2m-1}\frac{(1+m)^m}{m!^2}\\&<\varepsilon n^m(m+3).\end{aligned}$$

But, by [UB] (which is equivalent to [SP]), and Lemma 3.3

$$\left|\left(\frac{|I||J|}{n}\right)^m-|\sigma(I)\cap J|^m\right|<2^m\varepsilon n^m.$$

Since $m\geqslant 2$, this gives

$$\left|\mathbf{X}^{\tau}(\sigma|_K)-\frac{1}{m!^2}|\sigma(I)\cap J|^m\right|<\varepsilon n^m(m+4).$$

Finally, the fact that $\varepsilon\geqslant n^{-1}$ implies, as in (3),

$$\left|\binom{|\sigma(I)\cap J|}{m}-\frac{|\sigma(I)\cap J|^m}{m!}\right|\leqslant\varepsilon\frac{(1+m)^m}{m!}n^m,$$

so we may conclude

$$\left|\mathbf{X}^{\tau}(\sigma|_K)-\frac{1}{m!}\binom{|\sigma(I)\cap J|}{m}\right|<\varepsilon n^m(m+5).\qquad\square$$

Proposition 3.5. [mS] $\Rightarrow$ [2S].

Proof. Let $K=\sigma(I)\cap J$ for some intervals $I,J\in\mathbb{Z}_n$ with $|I|\geqslant n/2$ and $|J|\geqslant n/2$, and let $k=|K|$. It is easy to see that

$$\mathbf{X}^{(01)}(\sigma|_K)=\binom{k-2}{m-2}^{-1}\sum_{\pi\in S_m}\mathbf{X}^{(01)}(\pi)\mathbf{X}^{\pi}(\sigma|_K).$$

Therefore, applying [mS], we have

$$\mathbf{X}^{(01)}(\sigma|_K) = \binom{k-2}{m-2}^{-1}\left(\frac{1}{m!}\binom{k}{m} + o(n^m)\right)\sum_{\pi\in S_m}\mathbf{X}^{(01)}(\pi).$$

Since the last sum in this expression is $m!\cdot m(m-1)/4$ by symmetry, we may simplify to

$$\begin{aligned}\mathbf{X}^{(01)}(\sigma|_K) &= \frac{1}{2}\binom{k}{2} + \frac{m!^2\varepsilon n^m}{(n/4)^{m-2}(4+o(1))}\\ &= \frac{1}{2}\binom{k}{2} + 4^{m-1}m!^2\varepsilon n^2.\end{aligned}$$

We have $\mathbf{X}^{(01)}(\sigma|_K) + \mathbf{X}^{(10)}(\sigma|_K) = \binom{k}{2}$, so the result follows. □

Call a proper interval $I\subset\mathbb{Z}_n$ "contiguous" if I does not contain both 0 and $n-1$, "terminal" if its complement is contiguous, "initial" if it is terminal and contains 0, and "final" if it is terminal and contains $n-1$. We denote the complement of an interval I by $\bar{I}$.

Proposition 3.6. [2S] ⇒ [UB].

Proof. Suppose σ satisfies [2S] but not [UB]. We claim that, for infinitely many n and some $\varepsilon>0$, there are intervals $I,J\subset\mathbb{Z}_n$ with I and J initial, and $D_J(\sigma(I))$ at least $27\varepsilon n/2$. Since [UB] is not true for σ, we may choose ε so that there are proper subintervals $I,J\subset\mathbb{Z}_n$ with $D_J(\sigma(I))\geqslant 864\varepsilon n$. By taking complements, splitting sets into initial and final intervals, and taking unions, we may assume that I and J are terminal and have length $\geqslant n/2$. Doing so has the impact of dividing $D_J(\sigma(I))$ by 64 at most, so $D_J(\sigma(I))\geqslant 27\varepsilon n/2$. Since the other three cases are essentially identical, we assume that I and J are initial.

For ease of notation, we will let

$$\begin{aligned}A &= I\cap\sigma^{-1}(J) \quad a=|A|,\\ B &= I\cap\sigma^{-1}(\bar{J}) \quad b=|B|,\\ C &= \bar{I}\cap\sigma^{-1}(J) \quad c=|C|,\\ D &= \bar{I}\cap\sigma^{-1}(\bar{J}) \quad d=|D|.\end{aligned}$$

For subsets $S,T\subset\mathbb{Z}_n$, let $\partial_\sigma(S,T)$ denote the number of pairs $(x,y)\in S\times T$ such that $x<y$ and $\sigma(x)<\sigma(y)$. Then

$$\begin{aligned}\mathbf{X}^{(01)}(\sigma) &= \mathbf{X}^{(01)}(\sigma|_I) + \mathbf{X}^{(01)}(\sigma|_{\bar{I}}) + \partial_\sigma(I,\bar{I})\\ &= \mathbf{X}^{(01)}(\sigma|_I) + \mathbf{X}^{(01)}(\sigma|_{\bar{I}}) + \partial_\sigma(A,C)\\ &\quad + \partial_\sigma(A,D) + \partial_\sigma(B,C) + \partial_\sigma(B,D).\end{aligned}$$

Now, $\partial_\sigma(B,C)=0$ and $\partial_\sigma(A,D)=ad$, since every element of J is less than every element of $\bar{J}$, and every element of I is less than every element of $\bar{I}$. Also,

$$\partial_\sigma(A,C)=\mathbf{X}^{(01)}(\sigma|_{\sigma^{-1}(J)})-\mathbf{X}^{(01)}(\sigma|_A)-\mathbf{X}^{(01)}(\sigma|_C),$$
$$\partial_\sigma(B,D)=\mathbf{X}^{(01)}(\sigma|_{\sigma^{-1}(\bar{J})})-\mathbf{X}^{(01)}(\sigma|_B)-\mathbf{X}^{(01)}(\sigma|_D).$$

Thus, we have

$$\begin{aligned}\mathbf{X}^{(01)}(\sigma)=&\mathbf{X}^{(01)}(\sigma|_I)+\mathbf{X}^{(01)}(\sigma|_{\bar{I}})+\mathbf{X}^{(01)}(\sigma|_{\sigma^{-1}(J)})-\mathbf{X}^{(01)}(\sigma|_A)\\&-\mathbf{X}^{(01)}(\sigma|_C)+ad+\mathbf{X}^{(01)}(\sigma|_{\sigma^{-1}(\bar{J})})-\mathbf{X}^{(01)}(\sigma|_B)-\mathbf{X}^{(01)}(\sigma|_D).\end{aligned}$$

By [2S], for sufficiently large n, each term $\mathbf{X}^{(01)}(\sigma|_S)$ can be approximated by $\binom{|S|}{2}/2$ to within $\varepsilon n^2/2$, and therefore by $|S|^2/4$ to within $3\varepsilon n^2/4$, since

$$\left|\binom{|S|}{2}-\frac{|S|^2}{2}\right|=\frac{|S|}{2}\leqslant\frac{\varepsilon}{2}n^2.$$

Therefore, rewriting and multiplying by 4, we have that

$$|n^2-(a+b)^2-(c+d)^2-(a+c)^2-(b+d)^2+a^2+b^2+c^2+d^2-4ad|$$

is bounded above by $27\varepsilon n^2$. Since $n=a+b+c+d$, we may simplify down to

$$|bc-ad|<\frac{27\varepsilon}{2}n^2. \tag{4}$$

Let $\delta n=|I\cap\sigma^{-1}(J)|-|I||J|/n$. Then, since σ violates [UB],

$$\begin{aligned}|bc-ad|&=\left|\left(\frac{|I||\bar{J}|}{n}-\delta n\right)\left(\frac{|\bar{I}||J|}{n}-\delta n\right)-\left(\frac{|I||J|}{n}+\delta n\right)\left(\frac{|\bar{I}||\bar{J}|}{n}+\delta n\right)\right|\\&=|\delta|(|I||J|+|I||\bar{J}|+|\bar{I}||J|+|\bar{I}||\bar{J}|)\\&=\frac{D_J(\sigma(I))}{n}\cdot(|I|+|\bar{I}|)(|J|+|\bar{J}|)\geqslant\frac{27\varepsilon}{2}n^2\end{aligned}$$

contradicting (4). □

We present a simple application of these results. The following observation has some relevance to the investigations of [2,3].

Proposition 3.7. *If a permutation $\sigma\in S_n$ excludes $\tau\in S_m$ (in the sense that $\mathbf{X}^\tau(\sigma)=0$), where $n\geqslant m^3$, then*

$$D(\sigma)\geqslant n(m\cdot m!^4\cdot 4^{m-1})^{-1}.$$

Proof. Let $\varepsilon = D(\sigma)/n$. We show that, if

$$\varepsilon < (m \cdot m!^4 \cdot 4^{m-1})^{-1}$$

then there is at least one copy of every element τ of S_m in σ. According to the implication from [UB] to [mS], if $D(\sigma) \leqslant \varepsilon n$, then

$$\left| \mathbf{X}^{\tau}(\sigma) - \frac{1}{m!}\binom{n}{m} \right| < \frac{(m+5)4^{m-1}m!^2}{m \cdot m!^4 \cdot 4^{m-1}} n^m \leqslant \frac{1}{m!}\binom{n}{m},$$

so that $\mathbf{X}^{\tau}(\sigma) > 0$. □

Corollary 3.8. *There is a constant $c > 0$ so that, if $n \geqslant m^3$ and $\sigma \in S_n$ excludes $\tau \in S_m$, then*

$$\frac{D(\sigma)}{n} > (cm)^{-4m}.$$

4. A construction

In this section, we present a construction for a large class of permutations which are highly quasirandom. We will assume throughout that $\sigma \in S_n$ and $\tau \in S_m$, unless indicated otherwise.

Definition 4.1. For permutations $\sigma \in S_n$ and $\tau \in S_m$, considered as actions on $\mathbb{Z}_n$ and $\mathbb{Z}_m$, respectively, define $\sigma \otimes \tau \in S_{nm}$ by $(\sigma \otimes \tau)(x) = \tau(\lfloor \frac{x}{n} \rfloor) + m\sigma(x \bmod n)$. We will also denote the kth product of σ with itself as $\sigma^{(k)}$.

A special case of this product appears in [7], where the authors define a sequence of permutations lacking "monotone 3-term arithmetic progressions" by taking iterated products of the elements of S_2.

Note that $\sigma \otimes \tau$ has the property that $(\sigma \otimes \tau)([0, n-1])$ is the set of all elements of $\mathbb{Z}_{nm}$ congruent to 0 mod m (i.e., $m \cdot [0, n-1]$), a set which necessarily lacks the "weak translation" property of quasirandom sets. Thus, a sequence $\{\sigma_1, \sigma_1 \otimes \sigma_2, \sigma_1 \otimes \sigma_2 \otimes \sigma_3, \ldots\}$ sends intervals to sets which are not quasirandom in the sense of [5]. Nonetheless, we will prove shortly that it does satisfy UB. First, note that, since $x = an_1n_2 + bn_1 + c$ implies

$$[(\sigma_1 \otimes \sigma_2) \otimes \sigma_3](x) = \sigma_3(a) + n_3\sigma_2(b) + n_2n_3\sigma_1(c) = [\sigma_1 \otimes (\sigma_2 \otimes \sigma_3)](x)$$

the operation $\otimes$ is associative.

Define $d(\sigma)$ by

$$d(\sigma) = \max_{I,J} D_J(\sigma(I)),$$

where J is allowed to vary over all possible intervals, but I is restricted to initial intervals. We denote the analogue for final intervals by d'. Then we have the following result:

Proposition 4.2. $d(\sigma\otimes\tau)\leqslant m-1+d(\sigma)$.

Proof. Let the interval $I_k=[kn,(k+1)n-1]\subset\mathbb{Z}_{nm}$. Then, any initial interval S of $\mathbb{Z}_{nm}$ can, for some $l<m$, be written

$$S=\bigcup_{k=0}^{l} I_k\cup S_0,$$

where S_0 is an initial segment of I_{l+1}. For any interval $J\subset\mathbb{Z}_{nm}$, then, we may write

$$D_J((\sigma\otimes\tau)(S))\leqslant\sum_{k=0}^{l} D_J((\sigma\otimes\tau)(I_k))+D_J((\sigma\otimes\tau)(S_0))$$

by Lemma 2.1. First, we estimate $D_J(\sigma(I_k))$.

$$\begin{aligned}D_J((\sigma\otimes\tau)(I_k))&=\left|\,|(\sigma\otimes\tau)(I_k)\cap J|-\frac{|(\sigma\otimes\tau)(I_k)||J|}{nm}\right|\\&=\left|\,|(m[0,n-1]+k)\cap J|-\frac{n|J|}{nm}\right|\\&\leqslant\left|\frac{|J|+m-1}{m}-\frac{|J|}{m}\right|=\frac{m-1}{m}.\end{aligned}$$

Let $J_0\subset\mathbb{Z}_n$ denote the set $\{\lfloor\frac{x}{m}\rfloor\,|\,x\in J\}$, and let $S_1\subset\mathbb{Z}_n$ be the set S_0 reduced mod n. Then,

$$\begin{aligned}D_J((\sigma\otimes\tau)(S_0))&=\left|\,|(\sigma\otimes\tau)(S_0)\cap J|-\frac{|(\sigma\otimes\tau)(S_0)||J|}{nm}\right|\\&=\left|\,|\sigma(S_1)\cap J_0|-\frac{|S_1||J|}{nm}\right|\\&=\left|\,|\sigma(S_1)\cap J_0|-\frac{|S_1|m|J_0|}{nm}+\frac{|S_1|}{nm}(m|J_0|-|J|)\right|\\&\leqslant D_{J_0}(\sigma(S_1))+\left(\frac{n}{nm}(m-1)\right)\leqslant d(\sigma)+\frac{m-1}{m}.\end{aligned}$$

Thus,

$$\begin{aligned}d(\sigma\otimes\tau)&\leqslant(m-1)\frac{m-1}{m}+\frac{m-1}{m}+d(\sigma)\\&=m-1+d(\sigma).\qquad\square\end{aligned}$$

An identical result holds for d', by symmetry. We use this in the next proposition, which allows us to bound discrepancies recursively.

Proposition 4.3. $D(\sigma\otimes\tau)\leqslant m-1+d(\sigma)+d'(\sigma)$.

Proof. Note that every interval I of $\mathbb{Z}_{nm}$ is of the form

$$S = \bigcup_{k\in[l,L]} I_k \cup S_0 \cup S_0',$$

where $[l, L]$ is an interval of $\mathbb{Z}_m$ of length no more than $m-2$, S_0 is an initial segment of I_{L+1}, and S_0' is a final segment of I_{l-1}. Applying Lemma 2.1,

$$D_J((\sigma\otimes\tau)(S)) \leqslant \sum_{k=l}^{L} D_J((\sigma\otimes\tau)(I_k)) + D_J((\sigma\otimes\tau)(S_0)) + D_J((\sigma\otimes\tau)(S_0')).$$

By the arguments presented in the proof of the previous proposition,

$$D_J((\sigma\otimes\tau)(I_k)) \leqslant \frac{m-1}{m},$$
$$D_J((\sigma\otimes\tau)(S_0)) \leqslant d(\sigma) + \frac{m-1}{m},$$
$$D_J((\sigma\otimes\tau)(S_0')) \leqslant d'(\sigma) + \frac{m-1}{m}.$$

Thus,

$$D(\sigma\otimes\tau) \leqslant m - 1 + d(\sigma) + d'(\sigma). \qquad \square$$

If we apply these results to a product of permutations,

Corollary 4.4. *For $\sigma\in S_n$, $D(\sigma^{(k)}) < 2kn$.*

Corollary 4.4 provides us with a family of very strongly quasirandom permutations, since, if $N = n^k$, then $\sigma^{(k)} \in S_N$ and $D(\sigma^{(k)}) < O(\log N)$. Immediately one wonders whether permutations exist with discrepancies which grow slower than $\log N$. A theorem of Schmidt [14] answers this question in the negative, implying that the $D(\sigma^{(k)})$ are, in a sense, "maximally" quasirandom.

Theorem 4.5 (Schmidt). *Let $\{x_i\}_{i=0}^{N-1} \subset [0,1)$, and define*

$$D(m) = \sup_{\alpha\in[0,1)} |\{\{x_i\}_{i=0}^{m-1} \cap [0,\alpha)| - m\alpha|.$$

Then there exists an integer $n \leqslant N$ so that $D(n) > \log N/100$.

We may immediately conclude that discrepancies grow at least as fast as $\log N$.

Corollary 4.6. *For any $\sigma\in S_N$, $D(\sigma) > \log N/100 - 1$.*

Proof. Take $x_i = \sigma(i)/N$ in Theorem 4.5. Then there exists an $\alpha\in[0,1)$ and an $n\leqslant N$ so that

$$\left|\left|\frac{\sigma([0,n-1])}{N} \cap [0,\alpha)\right| - n\alpha\right| > \frac{\log N}{100}.$$

Defining $k = \lfloor \alpha N \rfloor$, we have

$$\left| |\sigma([0,n-1]) \cap [0,k]| - \frac{n(k+1)}{N} \right| + \left| \frac{n(k+1)}{N} - n\alpha \right| > \frac{\log N}{100}.$$

Therefore, if we let I and J vary over all intervals in $\mathbb{Z}_N$,

$$\max_{I,J} \left| |\sigma(I) \cap J| - \frac{|I||J|}{n} \right| > \frac{\log N}{100} - 1,$$

so that $D(\sigma) > \log N/100 - 1$. □

One might expect that the algebraic properties of quasirandom permutations, such as the number of cycles, should be approximately that of random permutations (in this case, $\log n$). However, we have the following counterexample. Let i_n be the identity permutation on $\mathbb{Z}_n$. Then $i_n^{(k)}$ is always an involution in S_{n^k}—and the sequence $\{i_n^{(k)}/n^k\}_{i=0}^{n-1} \subset [0,1)$ is an initial segment of the van der Corput sequence. In fact, under this interpretation, Corollary 4.4 can be considered a generalization of the classical theorem that the discrepancy of the van der Corput sequence is $O(\log N)$. (See, for example, [8] for a modern version of this result.)

5. Conclusion

The original motivation for this paper was a (still unanswered) question of Graham [10]. For a sequence of permutations $\sigma_j \in S_{n_j}$, let $\mathbf{P}(k)$ be the property of *asymptotic k-symmetry*: for each $\tau \in S_k$,

$$\left| X^\tau(\sigma_j) - \frac{\binom{n_j}{k}}{k!} \right| = o(n_j^k).$$

Note that this property is weaker than property [kS] of Theorem 3.1, which we will call *strong* asymptotic k-symmetry. Theorem 3.1 says that strong asymptotic k-symmetry implies strong asymptotic $(k+1)$-symmetry for any $k \geqslant 2$. Graham asks whether there exists an analogous N so that, for all $k > N$, $\mathbf{P}(k) \Rightarrow \mathbf{P}(k+1)$? At first it might seem like one is asking for too much. However, precisely this type of phenomenon occurs for graphs [6]. It turns out that, if we let $\mathbf{G}(k)$ be the property that all graphs on k vertices occur as subgraphs at approximately the same rate, then

$$\mathbf{G}(1) \Leftarrow \mathbf{G}(2) \Leftarrow \mathbf{G}(3) \Leftarrow \mathbf{G}(4) \Leftrightarrow \mathbf{G}(5) \Leftrightarrow \mathbf{G}(6) \Leftrightarrow \cdots$$

In particular, $\mathbf{G}(4)$ implies quasirandomness, which in turn implies $\mathbf{G}(k)$ for all k.

The fact that $\mathbf{P}(1) \nRightarrow \mathbf{P}(2)$ is trivial. To show that $\mathbf{P}(2) \nRightarrow \mathbf{P}(3)$, let $\sigma_n \in S_{2n}$ be the permutation which sends x to $x+n$. Then $X^{01}(\sigma_n) = 2n(2n-1)$, and $X^{10}(\sigma_n) = 4n^2$, so that $|X^{01}(\sigma_n) - X^{10}(\sigma_n)| = o((2n)^2)$. However, the pattern (021) *never* appears in σ_n. We have been unable to date to provide an analogous result for any $\mathbf{P}(k)$ with $k > 2$.

A second, very natural question is that of the existence of *perfect* m-symmetry: the property of having all subsequence statistics *precisely* equal to their expected values. That is, for $\sigma \in S_n$,

$$X^{\tau}(\sigma) = \frac{\binom{n}{k}}{k!}$$

for all $\tau \in S_m$. For this to occur, the number of permutations of length m must evenly divide $\binom{n}{m}$. Let $\mathbf{D}(m)$ be the property of an integer N that

$$m! \left| \binom{n}{m} \right.$$

It is easy to see that a permutation $\sigma \in S_n$ with perfect m-symmetry must have perfect m'-symmetry for any $m' \leqslant m$, so n must satisfy $\mathbf{D}(m')$ for all such m'. Let $h(m)$ be the least n for which this occurs. A quick calculation reveals that $h(2) = 4$, $h(3) = 9$, $h(4) = 64$, and $h(5) = 128$. In fact, there is a perfect 2-symmetric permutation on 4 symbols: 3012. A computer search reveals that there are exactly two 3-symmetric permutations on 9 symbols: 650147832 and its reverse, 238741056. No m-symmetric permutation is known for $m > 3$, and the question of whether such permutations exist remains open. We conjecture that an m-symmetric permutation on sufficiently many symbols exists for all m, and believe it likely that one exists on $h(m)$ symbols.

Acknowledgments

The author wishes to thank Fan Chung Graham and Ron Graham for their tremendous help in formulating and attacking the problems discussed above. He also thanks Chris Dillard, Robert Ellis, and Lei Wu for helpful discussions during the development of this work, and the referee for many astute recommendations and observations.

References

[1] N. Alon, Generating pseudo-random permutations and maximum flow algorithms, Inform. Process. Lett. 35 (1990) 201–204.
[2] N. Alon, E. Friedgut, On the number of permutations avoiding a given pattern, J. Combin. Theory Ser. A 89 (2000) 133–140.
[3] M. Bóna, The solution of a conjecture of Stanley and Wilf for all layered patterns, J. Combin. Theory Ser. A 85 (1999) 96–104.
[4] F.R.K. Chung, R.L. Graham, Quasi-random set systems, J. Amer. Math. Soc. 4 (1991) 151–196.
[5] F.R.K. Chung, R.L. Graham, Quasi-random subsets of Z_n, J. Combin. Theory Ser. A 61 (1992) 64–86.
[6] F.R.K. Chung, R.L. Graham, R.M. Wilson, Quasi-random graphs, Combinatorica 9 (1989) 345–362.
[7] J.A. Davis, R.C. Entringer, R.L. Graham, G.J. Simmons, On permutations containing no long arithmetic progressions, Acta Arith. 34 (1977/78) 81–90.
[8] H. Faure, Discrépance quadratique de suites infinies en dimension un, in: Théorie des nombres (Quebec, PQ, 1987), Vols. 207–212, de Gruyter, Berlin, 1989.

[9] W.T. Gowers, A new proof of Szemerédi's Theorem, Geometric and Functional Anal. 11 (2001) 465–588.
[10] R.L. Graham, personal communication.
[11] J.C. Lagarias, Well-spaced labelling of points in rectangular grids, SIAM J. Discrete Math. 13 (2000) 521–534.
[12] B.D. McKay, J. Morse, H.S. Wilf, The distributions of the entries of Young tableaux, J. Combin. Theory Ser. A 97 (2002) 117–128.
[13] H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc. 84 (1978) 957–1041.
[14] W.M. Schmidt, Irregularities of distribution VII, Acta Arith. 21 (1972) 45–50.