

**QUASIRANDOMNESS AND REGULARITY:
LECTURE NOTES IV**

JOSHUA N. COOPER

1. SUBSETS OF \mathbb{Z}_n .

One of the most beautiful, and useful, areas in which quasirandomness has been studied concerns the subsets of the (rational) integers modulo n , which we write \mathbb{Z}_n . We need a few items of notation before introducing the random-like properties we are interested in. First of all, for $x \in \mathbb{Z}_n$, let $e_n(x) = e^{2\pi i x/n}$. When n is understood, we simply write $e(x)$. Then, for a subset $S \subset \mathbb{Z}_n$, let the function $\chi_S : \mathbb{Z}_n \rightarrow \{0, 1\}$ denote the characteristic function of S , i.e., $\chi_S(x) = 0$ if $x \notin S$ and 1 otherwise. Also, $S + t = \{s + t : s \in S\}$, and $\#(S \subset T) = |\{x : S + x \subset T\}|$, or, informally, the “number of copies of S in T .” Note that $\#(S \subset T) = |\bigcap_{u \in S} (T - u)|$. Finally, we define G_S to be the graph with vertex set \mathbb{Z}_n so that $\{i, j\} \in E(G_S)$ iff $i + j \in S$. The following are our quasirandom properties for the “ambient set” $S \subset \mathbb{Z}_n$ with cardinality $s = |S|$. Where a “test set” T is involved, t denotes the cardinality of T .

P_1 . For all but $o(n)$ $x \in \mathbb{Z}_n$, $|S \cap (S + x)| = s^2/n + o(n)$.

P_2 . For all $T \subset \mathbb{Z}_n$ and all but $o(n)$ $x \in \mathbb{Z}_n$, $|S \cap (T + x)| = st/n + o(n)$.

$P_3(k)$. For all but $o(n^k)$ $U \subset \mathbb{Z}_n$ with $|U| = k$, $\#(U \subset S) = s^k/n^{k-1} + o(n)$.

$P_4(k)$. For all but $o(n)$ $x \in \mathbb{Z}_n$,

$$\sum_{u_1 + \dots + u_k = x} \prod_{j=1}^k \chi_S(u_j) = s^k/n + o(n^{k-1}).$$

P_5 . For all $j \in \mathbb{Z}_n \setminus \{0\}$,

$$\sum_{x \in S} e(jx) = o(n).$$

P_6 . The graph G_S is quasirandom.

$P_7(2t)$.

$$\sum_{x_1, \dots, x_{2t}} \chi_S(x_1 + x_2) \cdot \dots \cdot \chi_S(x_{2t-1} + x_{2t}) \chi_S(x_{2t} + x_1) = s^{2t} + o(n^{2t}).$$

P_8 . For all $T \subset \mathbb{Z}_n$,

$$\sum_{x, y} \chi_T(x) \chi_T(y) \chi_S(x + y) = st^2/n + o(n^2).$$

Theorem 1. For $k \geq 2$ and $t \geq 2$, $P_1 \Leftrightarrow P_2 \Leftrightarrow P_3(k) \Leftrightarrow P_4(k) \Leftrightarrow P_5 \Leftrightarrow P_6 \Leftrightarrow P_7(2t) \Leftrightarrow P_8$.

Note that, given our understanding of graph quasirandomness thus far, this theorem cannot possibly be true. In particular, the number of edges in the graph G_S is $n|S|/2$, and we have made no restriction on the size of the sets $|S|$. What is needed, then, is a generalization of graph quasirandomness to the case of $0 < p < 1$, that is, to model the graphs in the family $G(n, p)$, whose edges are chosen independently at random from a Bernoulli distribution with success probability p . To that end, we present the following list of properties.

$Q_1(s)$. For all graphs H on s vertices,

$$\#(H \sqsubset G) = n^s p^{e(H)} (1-p)^{\binom{n}{2} - e(H)} (1 + o(1)).$$

$Q_2(2t)$. $\#(C_{2t} \subset G) = (1 + o(1))(np)^{2t}$.

Q_3 . For each $S \subset V(G)$, $e(S) = \frac{p|S|^2}{2} + o(n^2)$.

Q_4 . $\sum_{x, y} ||N(x) \cap N(y)| - p^2 n| = o(n^3)$.

To show that these are equivalent, we appeal to the work we have already done in the case of $p = 1/2$. In particular, given a graph G on n vertices with “density” $p = e(G)/\binom{n}{2}$ define G^* to be a *random* graph constructed as follows: for each edge $e \in G$, $e \in G^*$, and for each edge $e \notin G$, $e \in G^*$ with probability $(1/2 - p)/(1 - p)$, independent of all other edges. We will assume that $p < 1/2$, as the other case is almost identical. Let b_{ij} denote a Bernoulli variable of probability $(1/2 - p)/(1 - p)$ corresponding to the edge $ij \notin G$. We claim that the above properties are equivalent to G^* being quasirandom.

Proof. We wish to show that $\#(H' \sqsubset G) = n^s p^{e(H')} (1-p)^{\binom{s}{2} - e(H')} (1 + o(1))$ for all H' on s vertices implies $\#(H \sqsubset G^*) = n^s 2^{-\binom{s}{2}} (1 + o(1))$ with high probability for some fixed H on s (ordered) vertices. To see this, let $m = e(H)$, so that

$$\begin{aligned}
 \mathbf{E}[\#(H \sqsubset G^*)] &= \mathbf{E} \left[\sum_{v_1, \dots, v_s \in V(G)} \prod_{\{i, j\} \in H} a_{G^*}(v_i, v_j) \right] \\
 &= \sum_{H' \subset H} \mathbf{E} \left[\sum_{H'=G[\mathcal{X}]} \prod_{\{i, j\} \in H \setminus H'} b_{ij} \prod_{\{i, j\} \in K_s \setminus H} (1 - b_{ij}) \right] \\
 &= \sum_{H' \subset H} \sum_{H'=G[\mathcal{X}]} \left(\frac{1-2p}{2-2p} \right)^{m-e(H')} \left(\frac{1}{2-2p} \right)^{\binom{s}{2}-m} \\
 &= \sum_{H' \subset H} \#(H' \subset G) \left(\frac{1-2p}{2-2p} \right)^{m-e(H')} \left(\frac{1}{2-2p} \right)^{\binom{s}{2}-m} \\
 &= \sum_{H' \subset H} n^s p^{e(H')} (1-p)^{\binom{s}{2}-e(H')} (2-2p)^{-\binom{s}{2}+e(H')} \\
 &\quad \cdot (1-2p)^{m-e(H')} + o(n^s) \\
 &= n^s 2^{-\binom{s}{2}} \sum_{H' \subset H} (2p)^{e(H')} (1-2p)^{m-e(H')} + o(n^s) \\
 &= n^s 2^{-\binom{s}{2}} \sum_{j=0}^m \binom{m}{j} (2p)^j (1-2p)^{m-j} + o(n^s) \\
 &= n^s 2^{-\binom{s}{2}} + o(n^s).
 \end{aligned}$$

It is easy to see (using Chernoff's inequality, for example), that the value of $\#(H \sqsubset G^*)$ is concentrated about its mean, and so the claim follows. For the reverse implication, we show that $\#(H' \sqsubset G^*) = n^s 2^{-\binom{s}{2}} (1 + o(1))$ with high probability for each H' on s (ordered) vertices implies that $\#(H \sqsubset G) = n^s p^{e(H)} (1-p)^{\binom{s}{2} - e(H)} (1 + o(1))$ for each fixed H on s vertices. Note that, by the above argument,

$$\begin{bmatrix} \mathbf{E}[\#(H_1 \sqsubset G^*)] \\ \vdots \\ \mathbf{E}[\#(H_{2^s} \sqsubset G^*)] \end{bmatrix} = \mathbf{M} \begin{bmatrix} \#(H_1 \sqsubset G) \\ \vdots \\ \#(H_{2^s} \sqsubset G) \end{bmatrix},$$

where H_1, \dots, H_{2^s} are all of the s -vertex graphs, and \mathbf{M} is the matrix with entries

$$m_{H_1 H_2} = \begin{cases} (1-2p)^{e(H_2)-e(H_1)}(2-2p)^{e(H_1)-\binom{s}{2}} & \text{if } H_1 \subset H_2 \\ 0 & \text{otherwise.} \end{cases}$$

Since this matrix is triangular, it is invertible. Since it is invertible, there is only one vector of values $\#(H_j \sqsubset G)$ for each corresponding vector of values $\mathbf{E}[\#(H_j \sqsubset G^*)]$. By the previous calculation, the fact that $\#(H_j \sqsubset G) = n^s p^{e(H)} (1-p)^{\binom{s}{2}-e(H)} (1+o(1))$ for all j gives $\mathbf{E}[\#(H_j \sqsubset G^*)] = n^s 2^{-\binom{s}{2}} + o(n^s)$ for all j . The stated implication then follows.

Now, for Q_3 . Suppose $\mathcal{X} \subset V(G)$ implies $e(\mathcal{X}) = p|\mathcal{X}|^2/2 + o(n^2)$. Then

$$\begin{aligned} \mathbf{E}[e_{G^*}(\mathcal{X})] &= e_G(\mathcal{X}) + \frac{1-2p}{2-2p} \left(\binom{|\mathcal{X}|}{2} - e_G(\mathcal{X}) \right) \\ &= p \frac{|\mathcal{X}|^2}{2} + \frac{1-2p}{2-2p} (1-p) \frac{|\mathcal{X}|^2}{2} + o(n^2) = \frac{|\mathcal{X}|^2}{4} + o(n^2). \end{aligned}$$

Again, by concentration, this gives the desired result. The converse also follows, because the above computation is reversible.

As for Q_4 , suppose that $\sum_{x,y} ||N(x) \cap N(y)| - p^2 n| = o(n^3)$. Then

$$\#(C_4 \subset G) = \sum_{x,y} |N(x) \cap N(y)|^2 = p^4 n^4 + o(n^4),$$

which implies $Q_2(4)$. On the other hand,

$$\begin{aligned} \#(C_4 \subset G) &= \sum_{x,y} |N(x) \cap N(y)|^2 \\ &\geq n^{-2} \left(\sum_{x,y} |N(x) \cap N(y)| \right)^2 \\ &= n^{-2} \left(\sum_z |N(z)|^2 \right)^2 \\ &\geq n^{-4} \left(\sum_z \deg(z) \right)^4 \\ &= n^{-4} (2e(G))^4 = p^4 n^4 + o(n^4). \end{aligned}$$

Therefore, by the standard ‘‘squeeze argument,’’ if $Q_2(4)$, then Q_4 .

Finally, $Q_2(2t)$. Clearly, $Q_1(t) \Rightarrow Q_2(2t)$, so that G^* being quasi-random implies $Q_2(2t)$, by the above. On the other hand, it is easy to see that $A^m = \mathcal{A}(G)^m$, the m^{th} power of G 's adjacency matrix encodes in its (v, w) -entry the number of length m (possibly self-intersecting) paths from v to w . Therefore, the trace $\text{tr}(A^{2t})$ counts the number of length $2t$ paths from a vertex to itself, i.e., the number of $2t$ -cycles. On the other hand,

$$(1) \quad \text{tr}(A^{2t}) = \sum_{j=1}^n \lambda_j^{2t} = (pn)^{2t} + o(n^{2t}),$$

which implies that $|\lambda_1| \leq pn + o(n)$. On the other hand, we can interpret $|\lambda_1|$ as the spectral radius of A , in which case

$$|\lambda_1| \geq \mathbf{a}^* A \mathbf{a}$$

for any unit vector \mathbf{a} . Taking $\mathbf{a} = \mathbb{1}/\sqrt{n} = (1, \dots, 1)/\sqrt{n}$ gives

$$|\lambda_1| \geq n^{-1} \sum_{v \in V(G)} \deg(v) = \frac{2e(G)}{n} \geq pn + o(n).$$

We may conclude that $\lambda_1 = pn + o(n)$ (since it is easy to see that $\lambda_1 \geq 0$), and, by (1), that $\lambda_2 = o(n)$.

Now, let \mathbf{a} be the characteristic vector of $S \subset V(G)$, and define \mathbf{e}_j to be the j^{th} vector in an orthonormal eigenbasis of A (corresponding to λ_j). Let $\mathbf{a}' = \mathbf{a} - (\mathbf{a} \cdot \mathbf{e}_1)\mathbf{e}_1$. Since $\mathbf{a}' \cdot \mathbf{e}_1 = 0$,

$$\mathbf{a}^* A \mathbf{a}' \leq |\lambda_2| |\mathbf{a}'|^2 \leq |\lambda_2| |\mathbf{a}|^2 = |\lambda_2| |S| = o(n) |S|.$$

On the other hand,

$$\begin{aligned} \mathbf{a}'^* A \mathbf{a}' &= \mathbf{a}^* A \mathbf{a} - 2(\mathbf{a} \cdot \mathbf{e}_1)(\mathbf{a}^* A \mathbf{e}_1) + (\mathbf{a} \cdot \mathbf{e}_1)^2 (\mathbf{e}_1^* A \mathbf{e}_1) \\ &= 2e(S) - \lambda_1 (\mathbf{a} \cdot \mathbf{e}_1)^2. \end{aligned}$$

We claim that $\mathbf{a} \cdot \mathbf{e}_1 = |S|/\sqrt{n} + o(\sqrt{|S|})$. To see this, let $\mathbf{u} = \mathbb{1}/\sqrt{n}$, and define $\mathbf{w} = \mathbf{e}_1 - \mathbf{u}$. We show below that $|\mathbf{w}| = o(1)$. Given this statement,

$$\mathbf{a} \cdot \mathbf{e}_1 = \mathbf{a} \cdot \mathbf{u} + \mathbf{a} \cdot \mathbf{w} = |S|/\sqrt{n} + O(|\mathbf{a}| |\mathbf{w}|) = |S|/\sqrt{n} + o(\sqrt{|S|}).$$

One may then conclude that

$$\mathbf{a}'^* A \mathbf{a}' = 2e(S) - (p + o(1)) |S|^2 + o(n^2) = o(n) |S|,$$

and so $e(S) = p|S|^2/2 + o(n^2)$, which is the content of Q_3 .

It remains only to show that $|\mathbf{w}| = o(1)$. Let $\mathbf{u} = \sum_j b_j \mathbf{e}_j$, so that $A \mathbf{u} = \sum_j b_j \lambda_j \mathbf{e}_j$. On the other hand, the j^{th} component of $A \mathbf{u}$ is

$\deg(v_j)/\sqrt{n}$, where v_j is the j^{th} vertex of G . Since

$$|\mathbf{A}\mathbf{u}| \leq \lambda_1 |\mathbf{u}| = \lambda_1,$$

we have $\sum_v \deg(v)^2 \leq p^2 n^3 + o(n^3)$. However, since

$$e(G) = \frac{1}{2} \sum_v \deg(v) \geq pn^2/2 + o(n^2),$$

we may apply Cauchy-Schwarz and conclude that

$$\sum_v |\deg(v) - pn| = o(n^2),$$

so that all but $o(n)$ components of $\mathbf{A}\mathbf{u}$ are $p\sqrt{n} + o(n^{1/2})$. Therefore, we may write

$$\mathbf{A}\mathbf{u} = (p + o(1)) \sqrt{n}\mathbf{u} + \mathbf{y}$$

where $|\mathbf{y}| = o(n)$. Then

$$\sum_{j=2}^n (\lambda_j - pn) b_j \mathbf{e}_j = \mathbf{y} + \mathbf{u} \cdot o(n)$$

and

$$\left(\sum_{j=2}^n (\lambda_j - pn)^2 b_j^2 \right)^{1/2} = o(n),$$

which, in turn, implies that $\sum_{j=2}^n b_j^2 = o(1)$. Since $|\mathbf{u} - b_1 \mathbf{e}_1| = o(1)$, and $|\mathbf{u}| = |\mathbf{e}_1| = 1$, we have $|b_1| = 1 + o(1)$. By the Perron-Frobenius Theorem, all the components of \mathbf{e}_1 are nonnegative, so $b_1 = 1 + o(1)$. \square

It is clear that $Q_1(s) \Leftrightarrow P_6$, $Q_2(2t) \Leftrightarrow P_7$, $Q_3 \Leftrightarrow P_8$, and $Q_4 \Leftrightarrow P_3(2)$ when $G = G_S$. It remains to show that

$$P_4(2) \Leftrightarrow P_4(k) \Leftrightarrow P_5 \Leftrightarrow P_2 \Leftrightarrow P_3(k) \Leftrightarrow P_3(2) \Leftrightarrow P_1.$$

Proof of $P_1 \Rightarrow P_2$. Let $T \subset \mathbb{Z}_n$. For all $a \in \mathbb{Z}_n$, we have, for almost all $b \in \mathbb{Z}_n$,

$$|(S - a) \cap (S - b)| = s^2/n + o(n).$$

Thus,

$$\sum_{a,b \in T} |(S - a) \cap (S - b)| = s^2 t^2/n + o(n^3),$$

which implies that

$$\sum_{a,b,x} \chi_S(x+a) \chi_S(x+b) \chi_T(a) \chi_T(b) = \sum_x \left(\sum_c \chi_S(x+c) \chi_T(c) \right)^2$$

$$= \sum_x |(S - x) \cap T|^2 = s^2 t^2 + o(n^3).$$

By Cauchy-Schwarz, this gives

$$n^{-1} \left(\sum_x |S \cap (T + x)| \right)^2 \leq \frac{s^2 t^2}{n} + o(n^3).$$

On the other hand, $\sum_x |S \cap (T + x)| = st$. Therefore, for almost all x , $|S \cap (T + x)| = st/n + o(n)$. \square

Proof of $P_2 \Rightarrow P_4(2)$. Let $T = -S$. Then, by P_2 , for almost all $x \in \mathbb{Z}_n$,

$$\sum_y \chi_S(y) \chi_T(y - x) = \sum_y \chi_S(y) \chi_S(x - y) = \frac{s^2}{n} + o(n),$$

which is precisely the content of $P_4(2)$. \square

Proof of $P_4(2) \Rightarrow P_4(k)$. We proceed by induction on k . The implication is trivial for $k = 2$. Assume that it holds for all $k' < k$ with $k \geq 3$. Then

$$\begin{aligned} & \sum_x \left(\sum_{u_1 + \dots + u_k = x} \chi(u_1) \cdots \chi(u_k) \right)^2 = \\ & \sum_x \left(\sum_y \chi(x - y) \sum_{u_2 + \dots + u_k = y} \chi(u_2) \cdots \chi(u_k) \right)^2 \\ & \sum_x \left(\sum_y \chi(x - y) \left(\frac{s^{k-1}}{n} + o(n^{k-2}) \right) \right)^2 + o(n^{2k-1}) \\ & \sum_x \left(\sum_y \chi(x - y) \right)^2 \left(\frac{s^{2k-2}}{n^2} + o(n^{2k-4}) \right) + o(n^{2k-1}) \\ & = s^2 n \cdot \frac{s^{2k-2}}{n^2} + o(n^{2k-1}) = \frac{s^{2k}}{n} + o(n^{2k-1}). \end{aligned}$$

This gives the desired result by Cauchy-Schwarz, since

$$\begin{aligned} & \sum_x \sum_{u_1 + \dots + u_k = x} \chi(u_1) \cdots \chi(u_k) = \\ & = \sum_x \sum_{u_1, \dots, u_{k-1}} \chi(u_1) \cdots \chi(u_{k-1}) \chi(x - \sum_{j=1}^{k-1} u_j) \end{aligned}$$

$$= \sum_{u_1, \dots, u_{k-1}} \chi(u_1) \cdots \chi(u_{k-1}) \sum_x \chi(x - \sum_{j=1}^{k-1} u_j) = s^k.$$

□

Proof of $P_4(k) \Rightarrow P_5$. Define the matrix $\mathbf{M} = (m_{ij})$, $i, j \in \mathbb{Z}_n$, by $m_{ij} = \chi(j - i)$. Then \mathbf{M} is circulant, and its eigenvalues are just the discrete Fourier coefficients of its first row, i.e.,

$$\lambda_j = \sum_{r \in S} e(jr).$$

On the other hand,

$$\begin{aligned} (\mathbf{M}^k)_{ij} &= \sum_{v_1, \dots, v_{k-1}} m_{i, v_1} m_{v_1, v_2} \cdots m_{v_{k-1}, j} \\ &= |\{v_1, \dots, v_{k-1} \mid \chi(v_1 - i) = \chi(v_2 - v_1) = \cdots = \chi(v_{k-1} - j)\}| \\ &= \sum_{u_1 + \dots + u_k = j - i} \prod_{q=1}^k \chi(u_q) = \frac{s^k}{n} + o(n^{k-1}), \end{aligned}$$

for almost all choices of i, j . Therefore,

$$\text{tr}((\mathbf{M}\mathbf{M}^*)^k) = s^{2k} + o(n^{2k}) = \sum_{i=0}^{n-1} \lambda_i^{2k}.$$

However, $\lambda_0 = s$, which immediately gives that $\lambda_j = o(n)$ for all $j \neq 0$, i.e., P_5 . □

Proof of $P_5 \Rightarrow P_1$. Suppose $\lambda_j = o(n)$ for all $j \neq 0$. Then,

$$\begin{aligned} \sum_{j \neq 0} |\lambda_j|^4 &\leq \max_{j \neq 0} |\lambda_j|^2 \sum_j |\lambda_j|^2 \\ &= o(n)^2 \cdot \sum_j \left| \sum_{r \in S} e(jr) \right|^2 \\ &= o(n)^2 \cdot \sum_j \left(\sum_{r_1, r_2 \in S} e(j(r_1 - r_2)) \right) \\ &= o(n)^2 \cdot ns = o(n^4). \end{aligned}$$

Also,

$$\sum_j |\lambda_j^4| = \sum_j \lambda_j^2 \bar{\lambda}_j^2$$

$$\begin{aligned}
 &= \sum_j \sum_{u_1, u_2, u_3, u_4 \in S} e(ju_1 + ju_2 - ju_3 - ju_4) \\
 &= \sum_j \sum_{u_1, u_2, u_3, u_4 \in S} e(j(u_1 + u_2 - u_3 - u_4)) \\
 &= n \cdot \left| \{(u_1, u_2, u_3, u_4) \in S^4 \mid u_1 - u_2 = u_3 - u_4\} \right|.
 \end{aligned}$$

On the other hand,

$$\begin{aligned}
 \sum_x |S \cap (S + x)|^2 &= \sum_x \sum_{u_1, u_2} \chi(u_1) \chi(u_2) \chi(u_1 - x) \chi(u_2 - x) \\
 &= \left| \{(u_1, u_2, u_3, u_4) \in S^4 \mid u_1 - u_3 = u_2 - u_4\} \right|,
 \end{aligned}$$

since we may take $u_3 = u_1 - x$ and $u_4 = u_2 - x$. Therefore,

$$\sum_x |S \cap (S + x)|^2 = n^{-1} \sum_j |\lambda_j^4| = n^{-1}(s^4 + o(n^4)) = \frac{s^4}{n} + o(n^3).$$

By Cauchy-Schwarz,

$$\sum_x |S \cap (S + x)|^2 \geq n^{-1} \left(\sum_x |S \cap (S + x)| \right)^2 = \frac{s^4}{n},$$

and, by the “squeeze argument,” this implies that $|S \cap (S + x)| = s^2/n + o(n)$ for almost all $x \in \mathbb{Z}_n$. \square

Proof of $P_2 \Rightarrow P_3(k)$. We proceed by induction on k . For $k = 2$, if we take $T = S$ in P_2 , one finds

$$\begin{aligned}
 \frac{s^2}{n} + o(n) &= |S \cap (S + x)| \\
 &= \sum_y \chi(y) \chi(y - x) \\
 &= \sum_z \chi(u_1 + z) \chi(u_2 + z),
 \end{aligned}$$

by taking $z = y - u_1$ and $u_2 = u_1 - x$, which is precisely the content of $P_3(k)$. Now, assume that the assertion holds for all values less than some $k \geq 3$. Let $U = \{u_1, \dots, u_k\} \subset \mathbb{Z}_n$, and define $T = \bigcap_{i=1}^{k-1} (S - u_i)$. By induction, $|T| = s^{k-1}/n^{k-2} + o(n)$. Now, apply P_2 to the sets S and T to get

$$\left| \bigcap_{i=1}^k (S - u_i) \right| = |T \cap (S - u_k)| = |(T + u_k) \cap S| = \frac{s^k}{n^{k-1}} + o(n).$$

\square

Proof of $P_3(k) \Rightarrow P_3(2)$. The result is obvious for $k = 2$. Assume that it holds for all values less than some $k \geq 3$. Then $P_3(k)$ gives

$$\begin{aligned}
\frac{s^{2k}}{n^{k-2}} + o(n^{k+2}) &= \sum_{u_1, \dots, u_k} \left(\sum_x \chi(x + u_1) \cdots \chi(x + u_k) \right)^2 \\
&= \sum_{u_1, u_2} \left(\sum_{u_3, \dots, u_k} \left(\sum_x \chi(x + u_1) \cdots \chi(x + u_k) \right)^2 \right) \\
&\geq \sum_{u_1, u_2} n^{2-k} \left(\sum_{u_3, \dots, u_k} \sum_x \chi(x + u_1) \cdots \chi(x + u_k) \right)^2 \\
&= n^{2-k} \sum_{u_1, u_2} (s^{2k-4} + o(n^{2k-4})) \left(\sum_x \chi(x + u_1) \chi(x + u_2) \right)^2
\end{aligned}$$

by induction and Cauchy-Schwarz. Thus,

$$\sum_{u_1, u_2} \left(\sum_x \chi(x + u_1) \chi(x + u_2) \right)^2 \leq s^4 + o(n^4).$$

However, since

$$\begin{aligned}
\sum_{u_1, u_2, x} \chi(x + u_1) \chi(x + u_2) &= \sum_x \left(\sum_{u_1} \chi(x + u_1) \right) \left(\sum_{u_1} \chi(x + u_2) \right) \\
&= s^2 n + o(n^3),
\end{aligned}$$

from which $P_3(2)$ follows by Cauchy-Schwarz. \square

Proof of $P_3(2) \Rightarrow P_1$. By $P_3(2)$, for almost all $u_1, u_2 \in \mathbb{Z}_n$,

$$\begin{aligned}
\frac{s^2}{n} + o(n) &= \sum_x \chi(x + u_1) \chi(x + u_2) \\
&= \sum_y \chi(y) \chi(y + u_2 - u_1) \\
&= |S \cap (S + u_1 - u_2)|.
\end{aligned}$$

\square