JOURNAL OF COMBINATORIAL THEORY, Series A, 61, 64–86 (1992)

Quasi-Random Subsets of $\mathbb{Z}_n$

F. R. K. CHUNG

Bell Communications Research, Morristown, New Jersey 07960

AND

R. L. GRAHAM

AT & T Bell Laboratories, Murray Hill, New Jersey 07974

Communicated by the Managing Editors

Received July 5, 1990

1. INTRODUCTION

It has been discovered in the past few years that there is a surprisingly large class $\mathcal{Q}$ of graph properties, all shared by random graphs, which are *equivalent* in the following sense: If a family of graphs satisfies *some* property in Q, then it must of necessity satisfy *all* the properties in Q. It was shown in [CGW89] (where these properties are termed *quasi-random*) that it is relatively easy to construct explicit families of graphs satisfying the quasi-random properties, which therefore imitate random graphs in many ways. Indeed, some of the most intransigent problems in combinatorics concern the explicit construction of graphs (and other combinatorial objects) satisfying particular properties known to be satisfied by almost all graphs of a particular size. For example, no one has yet come close to giving a construction for graphs on n vertices having no clique and no independent set of size more than $c \log n$, even though almost all graphs on n vertices have this property (for the value $c = 2$)! The best current construction, due to Frankl [Fr77] (also see [Ch81; FG85]) still only achieves $\exp(c\sqrt{\log n})$.

From this point of view, quasi-randomness offers a potential constructive alternative to the use of random graphs in certain circumstances. Previous results along these lines (providing much of the motivation for this work) can be found in Wilson [Wi72; Wi74], Erdös and Sós [ES82], Thomason [Th87a; Th87b; Th89], Haviland [Ha89], Haviland and Thomason [HT89], Rödl [Ro86], Frankl *et al.* [FRW88], Chung *et al.* [CGW89],

0097-3165/92 $5.00

Chung and Graham [CG90; CG90a; CG91; CGc], Chung [Ch90], Chung and Tetali [Ca], Spencer and Tetali [STa], and [STa], and Simonovits and Sós [SS91], where some of these papers deal with other structures besides graphs, such as matrices, hypergraphs, tournaments, and Boolean functions.

In this paper we extend this approach to subsets of $\mathbb{Z}_n$, the ring of integers modulo n. In particular, we describe a class of quasi-random properties for such subsets, relate these to quasi-random graph properties, and give explicit constructions for subsets satisfying these properties.

2. Notation

For $S \subset \mathbb{Z}_n$, the *indicator function* χ_S of S is defined by

$$\chi_S(z) = \begin{cases} 1 & \text{if } z \in S, \\ 0 & \text{otherwise.} \end{cases}$$

The *translate of S by x*, denoted by $S+x$, is the set $\{s+x \mid s \in S\}$, where here, as throughout the rest of the paper, addition of elements of $\mathbb{Z}_n$ is always performed modulo n. By $\#\{S \subset T\}$ we mean $|\{x \in \mathbb{Z}_n \mid S+x \subset T\}|$.

For $S \subset \mathbb{Z}_n$, the graph G_S has $\mathbb{Z}_n$ as its vertex set, and $\{\{i, j\} \mid i+j \in S\}$ as its edge set.

3. The Main Results

We next state a sequence of properties which a subset $S \subset \mathbb{Z}_n$ might possess. It will be noted that all of the properties we consider contain occurrences of the asymptotic "little oh" $o(\cdot)$ notation. In fact, each of these $o(1)$'s (for example) can be replaced by an appropriate function $f(n)$ which goes to 0 as $n \to \infty$. So to say that $P \Rightarrow P'$ for two of our properties means that if $S \subset \mathbb{Z}_n$ satisfies $P = P(f(n))$ then it also must satisfy $P' = P'(f'(n))$.

As usual, "almost all" $x \in X$, abbreviated as a.a. $x \in X$, means all except for $o(|X|)$ elements of X. We next list a collection of properties which might hold for subsets S, $T \subset \mathbb{Z}_n$, where $s := |S|$, $t := |T|$. We will often abbreviate χ_S by χ when S is understood.

Our primary result (Theorem 1) is that these properties are *equivalent*, i.e., any one implies any other.

(WT) *Weak translation.* For a.a. $x \in \mathbb{Z}_n$,

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

(ST) *Strong translation.* For all $T \subset \mathbb{Z}_n$ and a.a. $x \in \mathbb{Z}_n$,

$$|S \cap (T+x)| = st/n + o(n).$$

(P(2)) 2-*pattern.* For a.a. $u_1, u_2 \in \mathbb{Z}_n$,

$$\sum_x \chi(x+u_1)\,\chi(x+u_2) = s^2/n + o(n).$$

(P(k)) k-*pattern.* For a.a. $u_1, u_2, \ldots, u_k \in \mathbb{Z}_n$,

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

(R(2)) 2-*representation.* For a.a. $x \in \mathbb{Z}_n$,

$$\sum_{u_1+u_2=x} \chi(u_1)\,\chi(u_2) = s^2/n + o(n).$$

(R(k)) k-*representation.* For a.a. $x \in \mathbb{Z}_n$,

$$\sum_{u_1+\cdots+u_k=x} \prod_{i=1}^{k} \chi(u_i) = s^k/n^{k-1} + o(n).$$

(EXP) *Exponential sum.* For all $j \neq 0$ in $\mathbb{Z}_n$,

$$\sum_{x \in \mathbb{Z}_n} \chi(x) \exp\left(\frac{2\pi i j x}{n}\right) = o(n).$$

(GRAPH) *Quasi-random graph.* The graph G_S is quasi-random.

(C($2t$)) $2t$-*cycle.*

$$\sum_{x_1,\ldots,x_{2t}} \chi(x_1+x_2)\,\chi(x_2+x_3)\cdots\chi(x_{2t-1}+x_{2t})\,\chi(x_{2t}+x_1) = s^{2t} + o(n^{2t}).$$

(DENSITY) *Relative density.* 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 all subsets $S \subset \mathbb{Z}_n$, the preceding properties are equivalent.*

Proof. The flowchart shown in Fig. 1 will indicate the implications we will prove. The label ⓧ indicates that the corresponding implication is proved in Fact x.

Fact 1. (WT) ⇒ (ST).

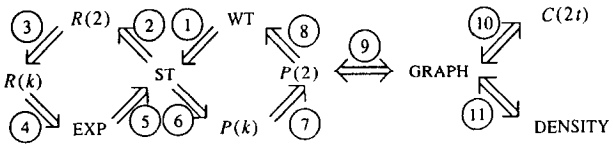

FIGURE 1

Let $T \subset \mathbb{Z}_n$. For all $a \in \mathbb{Z}_n$ we have by (WT) for almost all $b \in \mathbb{Z}_n$,

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

Thus,

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

so that

$$\begin{aligned} \sum_a \sum_b \sum_x \chi_S(x+a)\, \chi_S(x+b)\, \chi_T(a)\, \chi_T(b) \\ = \sum_{x \in \mathbb{Z}_n} \left(\sum_c \chi_S(x+c)\, \chi_T(c) \right)^2 \\ = \sum_x |(S-x) \cap T|^2 = s^2 t^2/n + o(n^3). \end{aligned}$$

Therefore, applying the Cauchy–Schwarz inequality, we have for a.a. $x \in \mathbb{Z}_n$,

$$|S \cap (T+x)| = st/n + o(n),$$

since

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

Fact 2. (ST) $\Rightarrow$ R(2).

In (ST), choose $T = -S$, so that $\chi_T(z) = \chi_S(-z)$. Thus, by (ST), a.a. $x \in \mathbb{Z}_n$ satisfy

$$\begin{aligned} \sum_{y \in \mathbb{Z}_n} \chi_S(y)\, \chi_T(y-x) &= \sum_y \chi_S(y)\, \chi_S(x-y) \\ &= s^2/n + o(n) \end{aligned}$$

which is just R(2).

Fact 3. $R(2) \Rightarrow R(k)$.

We proceed by induction on k. Of course, the assertion holds for $k=2$. Assume it holds for all values less than some fixed value of $k \geqslant 3$. Thus, we need to prove that for a.a. $x \in \mathbb{Z}_n$,

$$\sum_{u_1 + \cdots + u_k = x} \chi(u_1) \cdots \chi(u_k) = s^k/n + o(n^{k-1}). \tag{3.1}$$

Now,

$$\begin{aligned}
&\sum_x \Bigg(\sum_{u_1 + \cdots + u_k = x} \chi(u_1) \cdots \chi(u_k) \Bigg)^2 \\
&\quad = \sum_x \Bigg(\sum_{u_1 + y = x} \chi(u_1) \sum_{u_2 + \cdots + u_k = y} \chi(u_2) \cdots \chi(u_k) \Bigg)^2 \\
&\quad = \sum_x \Bigg(\sum_y \chi(x-y) \sum_{u_2 + \cdots + u_k = y} \chi(u_2) \cdots \chi(u_k) \Bigg)^2 \\
&\quad = \sum_x \Bigg(\sum_y \chi(x-y)(s^{k-1}/n + o(n^{k-2})) \Bigg)^2 + o(n^{2k-1}) \qquad \text{by induction} \\
&\quad = \sum_x \Bigg(\sum_y \chi(x-y) \Bigg)^2 (s^{2k-2}/n^2 + o(n^{2k-4})) + o(n^{2k-1}) \\
&\quad = s^{2k}/n + o(n^{2k-1})
\end{aligned}$$

which implies (3.1), since

$$\begin{aligned}
&\sum_x \sum_{u_1 + \cdots + u_k = x} \chi(u_1) \cdots \chi(u_k) \\
&\quad = \sum_x \sum_{u_1} \cdots \sum_{u_{k-1}} \chi(u_1) \cdots \chi(u_{k-1}) \chi(x - u_1 - \cdots - u_{k-1}) \\
&\quad = \sum_{u_1} \cdots \sum_{u_{k-1}} \sum_x \chi(x - u_1 - \cdots - u_{k-1}) \chi(u_1) \cdots \chi(u_{k-1}) = s^k + o(n^k).
\end{aligned}$$

Fact 4. $R(k) \Rightarrow (EXP)$.

Define the matrix $M = (m_{ij})$, $i, j \in \mathbb{Z}_n$, by $m_{ij} := \chi(j-i)$. Thus, M is a circulant and so has eigenvectors (e.g., see [Da79])

$$(1, \theta^l, \theta^{2l}, \ldots, \theta^{(n-1)l}), \qquad \theta = \exp(2\pi i l/n), \qquad l \in \mathbb{Z}_n,$$

with corresponding eigenvalues

$$\lambda_l := \sum_{x \in \mathbb{Z}_n} \chi(x)\, \theta^{lx}.$$

Now,

$$\begin{aligned}(M^k)_{i,j} &= \sum_{v_1, v_2, \ldots, v_{k-1}} m_{i,v_1} m_{v_1,v_2} \cdots m_{v_{k-1},j} \\ &= |\{v_1, \ldots, v_{k-1} | \chi(v_i - i) = \chi(v_2 - v_1) = \\ &\quad \cdots = \chi(j - v_{k-1}) = 1\}| \\ &= \sum_{u_1 + \cdots + u_k = j-i} \chi(u_1)\chi(u_2)\cdots\chi(u_k) = s^k/n + o(n^{k-1})\end{aligned}$$

for almost all choices of $j - i = x \in \mathbb{Z}_n$. Therefore,

$$\mathrm{Tr}(MM^{\mathrm{tr}})^k = s^{2k} + o(n^{2k}) = \sum_{i=0}^{n-1} \lambda_i^{2k}.$$

However,

$$\lambda_0 = \sum_x \chi_S(x) = s,$$

i.e.,

$$\lambda_0^{2k} = s^{2k}.$$

This implies for all $j \in \mathbb{Z}_n \setminus \{0\}$,

$$\lambda_j = \sum_x \chi_S(x) \exp\left(\frac{2\pi i j x}{n}\right) = o(n)$$

which is just (EXP).

Fact 5. (EXP) $\Rightarrow$ (ST).

Define, as before, the matrix $M = (m_{ij}) = (\chi(j-i))$. Thus M has eigenvalues $\lambda_j = \sum_x \chi(x) \exp(2\pi i j x/n)$, $j \in \mathbb{Z}_n$. Let $\lambda := \max_{j \neq 0} |\lambda_j|$. By hypothesis, $\lambda = o(n)$. Choose a fixed (arbitrary) $T \subset \mathbb{Z}_n$ of size $t := |T|$. Observe that if $s = o(n)$ or $t = o(n)$ then (ST) holds trivially. Hence, we may assume $s > \delta n$, $t > \delta n$ for some $\delta > 0$. Define $\bar{1} = (1, 1, \ldots, 1)^{\mathrm{tr}}$, the all 1's vector of length n,

$$\bar{\chi}_T = (\chi_T(0), \ldots, \chi_T(n-1))^{\mathrm{tr}}$$

and

$$\bar{v}_T = (v_T(0), \ldots, v_T(n-1))^{\mathrm{tr}}, \qquad \text{where } v_T(i) := \frac{1}{n-t}\left(-1 + \frac{n}{t}\chi(i)\right).$$

Thus,

$$\bar{\chi}_T = \frac{t(n-t)}{n}\left(\frac{1}{n-t} \cdot \bar{1} + \bar{v}_T\right),$$

where $\langle \bar{1}, \bar{v}_T \rangle = 0$. Also, we have

$$\|\bar{v}_T\| = \left(\frac{1}{t} + \frac{1}{n-t}\right)^{1/2} \tag{3.2}$$

and

$$M\bar{\chi}_T = \frac{st}{n} \cdot \bar{1} + \frac{t(n-t)}{n} M\bar{v}_T. \tag{3.3}$$

Now, *suppose* for some $\varepsilon > 0$,

$$\sum_x \left| |S \cap (T+x)| - \frac{st}{n} \right| > 3\varepsilon st. \tag{3.4}$$

Define

$$W := \left\{ y \,\middle|\, |S \cap (T+y)| - \frac{st}{n} \right| > \frac{\varepsilon st}{n} \Big\}.$$

Then $w := |W|$ must satisfy $w > 2\varepsilon s$, since otherwise we would have

$$\begin{aligned} \sum_{y \in \mathbb{Z}_n} \left| |S \cap (T+y)| - \frac{st}{n} \right| &= \sum_{y \in W} \left| |S \cap (T+y)| - \frac{st}{n} \right| \\ &\quad + \sum_{y \notin W} \left| |S \cap (T+y)| - \frac{st}{n} \right| \\ &\leqslant wt + \frac{\varepsilon st}{n} \cdot n \leqslant 3\varepsilon st, \end{aligned}$$

which contradicts (3.4).

We can assume without loss of generality (since the other case is essentially the same) that

$$W' = \left\{ y \in W \,|\, |S \cap (T+y)| > \frac{(1+\varepsilon)\, st}{n} \right\}$$

has $w' := |W'| > \varepsilon s$. Thus,

$$\sum_{y \in W'} |S \cap (T+y)| > (1+\varepsilon) \frac{stw'}{n}. \tag{3.5}$$

Let $W'' = -W'$ and define

$$\bar{\chi}_{W''} := (\chi_{W''}(0), \ldots, \chi_{W''}(n-1))^{\mathrm{tr}},$$

$$\bar{v}_{W''} := (v_0'', \ldots, v_{n-1}'')^{\mathrm{tr}}, \qquad \text{where} \quad v_i'' = \frac{1}{n-t}\left(-1 + \frac{n}{t} \chi_{W''}(i) \right).$$

As before,

$$\bar{\chi}_{W''} = \frac{w'(n-w')}{n}\left(\frac{1}{n-w'}\cdot\bar{1} + \bar{v}_{W''}\right)$$

with $\langle \bar{1}, \bar{v}_{W''}\rangle = 0$, and

$$\|\bar{v}_{W''}\| = \left(\frac{1}{w'} + \frac{1}{n-w'}\right)^{1/2}.$$

Therefore,

$$\begin{aligned}
\langle \bar{\chi}_{W''}, M\bar{\chi}_T\rangle &= \sum_{i,j} \chi_{W''}(i)\, m_{ij}\chi_T(j) \\
&= \sum_{i,j} \chi_{W''}(i)\,\chi_S(j-i)\,\chi_T(j) \\
&= \sum_{i\in W''} |T\cap(S+i)| \\
&= \sum_{y\in W'} |S\cap(T+y)| \geqslant \frac{(1+\varepsilon)\,stw'}{n} \qquad (3.6)
\end{aligned}$$

by (3.5). On the other hand,

$$\begin{aligned}
\langle \bar{\chi}_{W''}, M\bar{\chi}_T\rangle &= \left\langle \frac{w'}{n}\cdot\bar{1} + \frac{w'(n-w')}{n}\bar{v}_{W''}, \frac{st}{n}\cdot\bar{1} + \frac{t(n-t)}{n}M\bar{v}_T\right\rangle \\
&= \frac{w'st}{n} + \frac{w'(n-w')\,t(n-t)}{n^2}\langle \bar{v}_{W''}, M\bar{v}_T\rangle \\
&\leqslant \frac{w'st}{n} + \frac{w'(n-w')\,t(n-t)}{n^2}\lambda\|\bar{v}_{W''}\|\,\|\bar{v}_T\| \\
&\qquad \text{by the Courant–Fisher theorem (cf. [Ga77])} \\
&= \frac{w'st}{n} + \frac{w'(n-w')\,t(n-t)}{n^2}\cdot o(n) \\
&\quad \cdot\left(\frac{1}{t}+\frac{1}{n-t}\right)^{1/2}\left(\frac{1}{w'}+\frac{1}{n-w'}\right)^{1/2} \\
&= \frac{w'st}{n} + \frac{(w'(n-w')\,t(n-t))^{1/2}}{n}\cdot o(n) \\
&= \frac{w'st}{n} + o\left(\frac{w'st}{n}\right),
\end{aligned}$$

since $s > \delta n$, $t > \delta n$, and $w' > \varepsilon s$. This contradicts (3.6) and the proof of Fact 5 is complete.

Fact 6. $(\mathrm{ST}) \Rightarrow \mathrm{P}(k)$.

We proceed by induction on k. For $k=2$, property P(2) follows at once from property (ST) by choosing $T=-S$. Assume the assertion holds for all values less than some $k \geqslant 3$. Let $U=\{u_1, u_2, \ldots, u_k\} \subset \mathbb{Z}_n$. Define $T := \bigcap_{i=1}^{k-1} (S-u_i)$. By induction, $|T| = s^{k-1}/n^{k-2} + o(n)$. Now apply the assumption (ST) to the sets S and T. Thus,

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

This completes the induction step and Fact 6 is proved.

Fact 7. $\mathrm{P}(k) \Rightarrow \mathrm{P}(2)$.

The desired result is immediate for $k=2$. Assume that it holds for all values less than some $k \geqslant 3$. Then

$$\mathrm{P}(k) \Rightarrow \sum_{u_1,\ldots,u_k} \left(\sum_x \chi(x+u_1)\cdots\chi(x+u_k)\right)^2$$
$$= s^{2k}/n^{k-2} + o(n^{k+2})$$
$$= \sum_{u_1,u_2} \left\{ \sum_{u_3,\ldots,u_k} \left(\sum_x \chi(x+u_1)\cdots\chi(x+u_k)\right)^2 \right\}$$
$$\geqslant \sum_{u_1,u_2} \frac{1}{n^{k-2}} \left(\sum_{u_3,\ldots,u_k} \sum_x \chi(x+u_1)\cdots\chi(x+u_k)\right)^2$$

by the Cauchy–Schwarz inequality

$$= \frac{1}{n^{k-2}} \sum_{u_1,u_2} ((s^{k-2} + o(n^{k-2})) \left(\sum_x \chi(x+u_1)\,\chi(x+u_2)\right)^2$$

by the induction assumption. Thus,

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

However, since

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

then P(2) follows.

Fact 8. P(2) $\Rightarrow$ (WT).

Since P(2) $\Rightarrow$ for a.a. $u_1, u_2 \in \mathbb{Z}_n$,

$$\sum_x \chi_S(x+u_1)\,\chi_S(x+u_2) = s^2/n + o(n)$$

$$= \sum_y \chi_S(y)\,\chi_S(y+u_2-u_1)$$

$$= |S \cap (S+u_2-u_1)|$$

then (WT) follows.

Fact 9. P(2) $\Leftrightarrow$ (GRAPH).

Suppose P(2) holds for some subset $S \subset \mathbb{Z}_n$. Thus, a.a. choices of $u_1, u_2 \in \mathbb{Z}_n$ satisfy

$$\sum_x \chi_S(x+u_1)\,\chi_S(x+u_2) = s^2/n + o(n). \tag{3.7}$$

However, in the graph $G(S)$, the sum in (3.7) just counts $|nd(u_1) \cap nd(u_2)|$, where $nd(u)$ denotes the number of vertices in $G(S)$ which are adjacent to u. A straightforward extension of a result in [CGW89] asserts that the condition:

$$\sum_{u_1, u_2} \big||nd(u_1) \cap nd(u_2)| - s^2 n\big| = o(n^3) \tag{3.8}$$

is a quasi-random graph property. Since (3.7) and (3.8) are equivalent then Fact 9 follows.

The remaining two conditions, C(2t) and (DENSITY) are simply translations of quasi-random graph properties in [CGW89] into the corresponding results for subsets of $\mathbb{Z}_n$ (where, as in Fact 9, the graph properties need to be extended to the case of a *general* edge probability p from the standard case of $p = \frac{1}{2}$), We state these two graph properties for a family $\mathcal{G} = \{G(n)\}$ of graphs, where $G(n)$ has n vertices and $e(G(n))$ edges. For fixed $t \geq 2$, let $\#\{C_{2t} \subset G(n)\}$ denote the number of (ordered) $2t$-cycles in $G(n)$. Also, for a subset $X \subset V$, the vertex set of $G(n)$, let $e(X)$ denote the number of edges of $G(n)$ spanned by X. Let $0 < p < 1$ be fixed.

Fact 10. The condition

$$e(G(n)) = (1+o(1))\frac{pn^2}{2}, \quad \text{and} \quad \#\{C_{2t} \subset G(n)\} = (1+o(1))(pn)^{2t}$$

is a quasi-random graph property.

Fact 11. The condition

$$\text{For all } X \subset V, \quad \text{and} \quad e(X) = \frac{p}{2}|X|^2 + o(n^2)$$

is a quasi-random graph property.

It is not difficult to see that conditions C(2t) and (DENSITY) are immediate consequences of these. This completes the proof of Theorem 1. ∎

Sets S (or strictly speaking, families of sets with size tending to infinity) which satisfy any one, and therefore all, of the conditions of Theorem 1 will be called quasi-random.

4. Remarks on Related Results

Let $A = (a_n)$ be an infinite sequence of integers. For an integer m, we say that A is *uniformly distributed modulo m* (abbreviated u.d. (mod m)) if for every $j \in \mathbb{Z}_m$,

$$\lim_{N \to \infty} \frac{1}{N} |\{a_n \leqslant N \mid a_n \equiv j (\text{mod } m)\}| = \frac{1}{m}. \tag{4.1}$$

Also, A is said to be *uniformly distributed in* $\mathbb{Z}$ if A is u.d. (mod m) for all m (see [KN74] for a thorough discussion of these concepts). One characterization of sequences $A = (a_n)$ which are uniformly distributed in $\mathbb{Z}$ (abbreviated u.d. in $\mathbb{Z}$) is the following.

Theorem [KN74]. *$A = (a_n)$ is u.d. in $\mathbb{Z}$ if and only if for all $m \geqslant 2$,*

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \exp\left(\frac{2\pi i j a_n}{m}\right) = 0 \qquad \textit{for all} \quad j \in \mathbb{Z}_m \setminus \{0\}. \tag{4.2}$$

Note that this condition is rather similar to the condition (EXP). They are related as follows. For $S \subset \mathbb{Z}_n$ and $j \in \mathbb{Z}_m$ with m fixed, define the quantity

$$N_S(j) := |\{x \in S \mid x \equiv j \,(\text{mod } m)\}|.$$

In one direction we have the following.

Proposition 1. *If S is quasi-random then for all $j \in \mathbb{Z}_m$,*

$$N_S(j) = \frac{s}{m} + o(n). \tag{4.3}$$

Proof. Suppose for some $m \geqslant 2$ that (4.3) does not hold. Thus, we can assume without loss of generality that for a fixed $\varepsilon > 0$, the residue 0 modulo m occurs at least $(1/m + \varepsilon)s$ times where (as usual) we can assume that $s > \delta n$ for a fixed $\delta > 0$. Let us show that condition (ST) is violated. To do this, select $T = \{0, m, 2m, (\lfloor n/m \rfloor - 1)\, m\} \subset \mathbb{Z}_n$. Choose $\eta = \varepsilon s/2n$ and consider the ηn translates $T + jm$, $0 \leqslant j \leqslant \eta n$. A short calculation shows that for each such j,

$$|S \cap (T + jm)| \geqslant \left(\frac{1}{m} + \frac{\varepsilon}{2}\right) s \geqslant \left(\frac{1}{m} + \eta\right) s.$$

Since $\eta \geqslant \varepsilon\delta/2 > 0$ is independent of n, and $t := |T| = n/m + o(n)$ then (ST) is violated. ∎

We should point out that the converse does *not* hold, however. One example showing this is given by the set $S_{4n} = \{0, 2, ..., 2n-2, 2n+1, 2n+3, ..., 4n-1\} \subseteq \mathbb{Z}_{4n}$. For m fixed, it is easy to see that for all $j \in \mathbb{Z}_m$,

$$N_{S_{4n}}(j) = (1 + o(1))(2n/m).$$

On the other hand, S_{4n} does not satisfy the quasi-random property P(2). To see this, consider the two-point patterns $\{0, 2u+1\}$, $0 \leqslant u < \xi n$ for a small fixed $\xi > 0$. A simple calculation shows that each of these ξn patterns occurs at most $2\xi n$ times, violating P(2) (strongly).

One natural way to form sets from an infinite sequence $A = (a_k)$ is the following. For the integer n, define

$$S_n := \{a_m \in A \mid a_m < n\} \subset \mathbb{Z}_n.$$

One reason why S_n might not be quasi-random even though A is u.d. in $\mathbb{Z}$ is because A does not have an asymptotic density; that is, $\delta(A) := \lim_{N \to \infty} (1/N)|\{a_n \in A \mid a_n \leqslant N\}|$ does not exist. However, even if $\delta(A)$ exists, S_n can fail to be quasi-random, as the following example shows.

EXAMPLE. Let $\phi := (1 + \sqrt{5})/2$ and define $A^* = (a_0^*, a_1^*, a_2^*, ...)$, where

$$a_n^* := \lfloor n\phi \rfloor.$$

Let F_m denote the mth Fibonacci number, defined by

$$F_0 = 0, \qquad F_1 = 1, \qquad F_{r+2} = F_{r+1} + F_r, \qquad r \geqslant 0.$$

Finally, define

$$S_k^* := \{a_0^*, a_1^*, ..., a_{F_{2k-1}}^*\}.$$

It is not difficult to verify the following facts (e.g., see [GKP89]):

(i) $S_k^* \subset \mathbb{Z}_{F_{2k+1}}$;

(ii) $\{jF_{2k} (\mathrm{mod}\ F_{2k+1}) : 0 \leqslant j < F_{2k}\} = S_k^*$

(iii) $F_{2k-1}F_{2k} \equiv 1 \ (\mathrm{mod}\ F_{2k+1})$.

Now, A^* is u.d. in $\mathbb{Z}$ by Theorem 1.5 of [KN74]. (In fact, any sequence of the form $(\lfloor n\alpha \rfloor)$, α irrational, is u.d. in $\mathbb{Z}$.) Also, $\delta(A^*) = 1/\phi$. However, the set S_k^* is not quasi-random. To see this, we check that (EXP) is violated for the choice $j = F_{2k-1}$. Indeed, we have

$$\begin{aligned}
&\lim_{k\to\infty} \frac{1}{F_{2k+1}} \left| \sum_{x \in \mathbb{Z}_{F_{2k+1}}} \chi_{S_k^*}(x) \exp\left(\frac{2\pi i x F_{2k-1}}{F_{2k+1}}\right)\right| \\
&\quad = \lim_{k\to\infty} \frac{1}{F_{2k+1}} \left| \sum_{0 \leqslant j < F_{2k}} \exp\left(\frac{2\pi i j}{F_{2k+1}}\right)\right| \qquad \text{by (ii)} \\
&\quad = \lim_{k\to\infty} \frac{1}{F_{2k+1}} \left| \frac{1 - \exp(2\pi i F_{2k}/F_{2k+1})}{1 - \exp(2\pi i/F_{2k+1})}\right| \\
&\quad = \frac{1}{\pi} \sin\frac{\pi}{\phi} = 0.296675\ldots > 0,
\end{aligned}$$

which shows that S_k^* is not quasi-random.

Thus, while the concepts of quasi-randomness and uniform distribution in $\mathbb{Z}$ are related, they are in fact rather different.

Finally, we remark that for any $S \subset \mathbb{Z}_n$, since

$$\hat{\chi}_S(j) := \frac{1}{n} \sum_{x \in \mathbb{Z}_n} \chi_S(s) \exp\left(\frac{2\pi i j x}{n}\right)$$

is just the Fourier transform of χ_S, then by the Plancherel formula (e.g., see [Se77]), we have

$$\begin{aligned}
\sum_{j \in \mathbb{Z}_n} |\hat{\chi}_S(j)|^2 &= \sum_{j \in \mathbb{Z}_n} \left| \frac{1}{n} \sum_{x \in \mathbb{Z}_n} \chi_S(x) \exp\left(\frac{2\pi i j x}{n}\right)\right|^2 \\
&= \frac{1}{n} \sum_{x \in \mathbb{Z}_n} |\chi_S(x)|^2 = s/n;
\end{aligned}$$

i.e.,

$$\sum_{j=1}^{n-1} \left| \sum_{x \in \mathbb{Z}_n} \chi_S(x) \exp\left(\frac{2\pi i j x}{n}\right)\right|^2 = s(n-s). \tag{4.4}$$

However, for $s > \sigma n$, with $\sigma > 0$, (EXP) requires that each term of (4.4) has size $o(n^2)$; i.e., no unusual clustering can occur.

5. Restrictions of Quasi-Random Sets

Suppose for a fixed $\delta > 0$ we take $m > \delta n$ and restrict a quasi-random set $S \subset \mathbb{Z}_n$ to the set $S' = S \cap [0, m) \subset \mathbb{Z}_m$. Is S' also quasi-random? The answer turns out to be in the affirmative, and this forms the topic of this section. In order to prove this we first need the following preliminary result, which essentially asserts that if S is quasi-random then S' has nearly the same density as S, i.e., $s' := |S'|$ satisfies

$$\frac{s'}{m} = \frac{s}{n} + o(1).$$

(As usual, we can restrict ourselves to the case that $s \neq o(n)$, since the results hold trivially otherwise.) More precisely, consider the following two conditions (where $0 < \varepsilon < \delta$):

> For all $T \subset \mathbb{Z}_n$, with $t := |T|$, and for all except at most εn $x \in \mathbb{Z}_n$,
>
> $$\left| |S \cap (T + x)| - \frac{st}{n} \right| < \varepsilon n; \tag{5.1}$$
>
> $$\left| \frac{s}{n} - \frac{s'}{m} \right| < 20 \frac{n^3}{m^2 s} \sqrt{\varepsilon}. \tag{5.2}$$

Lemma. (5.1) $\Rightarrow$ (5.2).

Proof. It will be enough to prove that for $m \leqslant n/2$, (5.1) implies

$$\left| \frac{s}{n} - \frac{s'}{m} \right| \leqslant 10 \frac{n^3}{m^2 s} \sqrt{\varepsilon}. \tag{5.2}'$$

Assume the contrary, and in particular, assume that (5.1) holds but we have

$$\frac{s'}{m} - \frac{s}{n} \geqslant 10 \frac{n^3}{m^2 s} \sqrt{\varepsilon} \tag{5.3}$$

(the other case is similar and is omitted). Then, straightforward calculation gives

$$s - s' \leqslant \frac{(n-m)s}{n} \left(1 - 10 \frac{n^2}{m} \sqrt{\varepsilon} \right) \tag{5.4}$$

and

$$\frac{s'}{m} - \frac{s - s'}{n - m} > 10 \frac{n^3}{m^2 s} \sqrt{\varepsilon}. \tag{5.5}$$

Let Q denote an interval of length $\sqrt{\varepsilon}\, n$ in $[0, m)$ and define $Q' = Q \cap S$, where $q' := |Q'|$. By (5.1) for all except at most εn, $x \in \mathbb{Z}_n$, we have

$$\left| |S \cap (Q' + x)| - \frac{sq'}{n} \right| < \varepsilon n.$$

Define

$$P_{Q'} := \{x \in \mathbb{Z}_n \mid (Q' + x) \cap [0, m) = \varnothing\}.$$

Note that $|P_{Q'}| = n - m - \sqrt{\varepsilon}\, n$.

We next consider the following sum over *all* intervals Q of length $\sqrt{\varepsilon}\, n$ in $[0, m)$ (with $Q' = Q \cap S$):

$$\sum_{Q', x \in P_{Q'}} \left| |S \cap (Q' + x)| - \frac{sq'}{n} \right| < m(n-m)\, \varepsilon n + m \cdot \varepsilon n \cdot m < 2\varepsilon mn^2. \tag{5.6}$$

On the other hand, now consider an interval R of length $\sqrt{\varepsilon}\, n$ in $[m, n)$, and set $R' = R \cap S$, $r' := |R'|$. Again, by (5.1), for all except at most εn $y \in \mathbb{Z}_n$,

$$\left| |S \cap (R' + y)| - \frac{sr'}{n} \right| < \varepsilon n.$$

Define

$$P'_{R'} := \{y \in \mathbb{Z}_n \mid (R' + y) \subset [0, m)\}.$$

Note that $|P'_{R'}| = m - \sqrt{\varepsilon}\, n$. Thus, summing over all such R (with $R' = R \cap S$), we have

$$\sum_{R', y \in P_{R'}} \left| |S \cap (R' + y)| - \frac{sr'}{n} \right| < (n-m)\, m \cdot \varepsilon n + (n-m) \cdot \varepsilon n \cdot m < 2\varepsilon mn^2. \tag{5.7}$$

Now, since

$$\sum_{Q', x \in P_{Q'}} |S \cap (Q' + x)| = \sum_{R', y \in P'_{R'}} |S \cap (R' + y)|$$

(both sums count the total number of intersections of an interval in $[0, m)$ with a translated interval from $[m, n)$), then by (5.6) and (5.7) we obtain

$$\left| (n - m - \sqrt{\varepsilon}\, n) \sum_{Q'} \frac{sq'}{n} - (m - \sqrt{\varepsilon}\, n) \sum_{R'} \frac{sr'}{n} \right| < 4\varepsilon mn^2$$

i.e.,

$$\frac{s}{n}\left|(n-m)\sum_{Q'} q' - m\sum_{R'} r'\right| < 6\varepsilon mn^2. \tag{5.8}$$

Since

$$\left|\sum_{Q'} q' - \sqrt{\varepsilon}\, ns'\right| \leqslant 2\sqrt{\varepsilon}\, n \cdot \sqrt{\varepsilon}\, n = 2\varepsilon n^2$$

and

$$\left|\sum_{R'} r' - \sqrt{\varepsilon}\, n(s-s')\right| \leqslant 2\sqrt{\varepsilon}\, n \cdot \sqrt{\varepsilon}\, n = 2\varepsilon n^2$$

then we have from (5.8),

$$sm(n-m)\sqrt{\varepsilon}\left|\frac{s'}{m} - \frac{s-s'}{n-m}\right| \leqslant 10\varepsilon n^2;$$

i.e.,

$$\left|\frac{s'}{m} - \frac{s-s'}{n-m}\right| \leqslant \frac{10n^3\sqrt{\varepsilon}}{sm(n-m)} < \frac{10n^3\sqrt{\varepsilon}}{sm^2},$$

since we are assuming $m < n/2$. However, this contradicts (5.4), and the lemma is proved. ∎

THEOREM 2. *If $S \subset \mathbb{Z}_n$ is quasi-random and $S' = S \cap [0, m) \subset \mathbb{Z}_m$ with $m > \delta n$, $\delta > 0$ fixed, then S' is quasi-random.*

Proof. We will show that if S satisfies (5.1) then it also satisfies the following form of (WT):

$$\sum_{x \in \mathbb{Z}_m}\left||S' \cap (S'+x)| - \frac{(s')^2}{m}\right| \leqslant \frac{22n^3\sqrt{\varepsilon}}{s}. \tag{5.9}$$

In applying (5.1) we will choose T to be of the form $S \cap [a, b)$ for various intervals $[a, b) \subset \mathbb{Z}_n$. We first partition $[0, m)$ into $l = 1/\sqrt{\varepsilon}$ disjoint intervals $I_1, \ldots, I_l$, each of length essentially $\sqrt{\varepsilon}\, m$. Let T_i denote $I_i \cap S'$ and $t_i := |T_i|$. Clearly, for each fixed $x \in \mathbb{Z}_m$,

$$|S' \cap (S'+x)| = \left|S' \cap \left(\bigcup_i (T_i + x)\right)\right|$$

$$= \sum_i |S' \cap (T_i + x)|$$

(where addition is taken in $\mathbb{Z}_m$).

Observe that $S' \cap (T_i + x) \pmod m$ and $S \cap (T_i + x) \pmod n$ consist of the same elements except possibly for a single index i. Therefore by (5.1), all but at most εn of the $x \in \mathbb{Z}_m$ satisfy

$$\left| |S' \cap (T_i + x)| - \frac{st_i}{n} \right| < \varepsilon n \qquad \text{for all but at most one index } i.$$

By the lemma we have

$$\left| \frac{s}{n} - \frac{s'}{m} \right| < \frac{20n^3}{m^2 s} \sqrt{\varepsilon}.$$

Thus, we obtain for these x,

$$\left| |S' \cap (T_i + x)| - \frac{t_i s'}{m} \right| < \varepsilon n + \frac{20n^3 t_i}{m^2 s} \sqrt{\varepsilon}. \tag{5.10}$$

Consequently, by (5.10),

$$\begin{aligned}
&\sum_{x \in \mathbb{Z}_m} \left| |S' \cap (S' + x)| - \frac{(s')^2}{m} \right| \\
&\quad \leqslant \sum_{x \in \mathbb{Z}_m} \sum_i \left| |S' \cap (T_i + x)| - \frac{(s')^2}{m} \right| \\
&\quad \leqslant \sum_{x,i} \left| |S' \cap (T_i + x)| - \frac{t_i s'}{m} \right| \\
&\quad \leqslant \frac{1}{\sqrt{\varepsilon}} m \cdot \varepsilon n + m \cdot \frac{20n^3 m}{m^2 s} \sqrt{\varepsilon} + m^2 \sqrt{\varepsilon} \\
&\quad \leqslant 22 \frac{n^3}{s} \sqrt{\varepsilon},
\end{aligned}$$

as claimed. This completes the proof of Theorem 2. ∎

Since S quasi-random implies $S + t$ is quasi-random for all $t \in \mathbb{Z}_n$, thus in fact Theorem 2 holds when $[0, m)$ is replaced by any interval of length m. More generally, the same general results hold if we interact S with a bounded number of disjoint intervals of total length m, and concatenate them where some may have been reflected to form a subset of $\mathbb{Z}_m$. Also, one can get other quasi-random sets S' for S by defining $\chi_{S'}(i) = \chi_S(c + di)$, $0 \leqslant i < m$, where $m > \delta n$ and g.c.d. $(d, n) = o(n)$.

6. Examples of Quasi-Random Sets

A standard example for exhibiting random-like behavior with a well-defined structure is to use the quadratic residues modulo some prime (e.g., see [GS71; BT81; CGW89]). For us, this means forming the subset

$$Q_p = \{x^2 \mid x \in \mathbb{Z}_p,\ p \text{ prime}\} \subset \mathbb{Z}_p.$$

There are many ways of showing that Q_p is quasi-random. One is to check the (EXP) condition. In this case,

$$\sum_{x \in \mathbb{Z}_p} \chi_{Q_p}(x) \exp\left(\frac{2\pi i j x}{p}\right) = \frac{1}{2} \sum_{x \in \mathbb{Z}_p} \exp\left(\frac{2\pi i j x^2}{p}\right) \tag{6.1}$$

which is closely related to Gauss sums modulo p (see [IR72]). In particular, it is known that for any $j \not\equiv 0 \pmod p$, the sum in (6.1) is $O(p^{1/2})$, which implies that (EXP) holds for Q_p. This construction is actually a special case of the following general situation. For a fixed integer $r > 0$, let $p = mr + 1$ be prime and let $A \subset \mathbb{Z}_p^*$ consist of t non-zero residues which belong to distinct rth power characters modulo p, i.e., for any distinct $a, b \in A$, ab^{-1} is not an rth power in $\mathbb{Z}_p^*$. Let $Q_r = \{x^r \mid x \in \mathbb{Z}_p^*\}$ denote the rth powers in $\mathbb{Z}_p^*$ and define

$$S = AQ_r = \{aq \mid a \in A,\ q \in Q_r\} \subset \mathbb{Z}_p.$$

We claim that S is quasi-random. To see this, we check the (EXP) condition. Thus, for $\zeta = e^{2\pi i/p}$, $j \not\equiv 0$,

$$\begin{aligned}
\left|\sum_{x \in \mathbb{Z}_p} \chi_S(x)\, \zeta^{jx}\right| &= \frac{1}{r}\left|\sum_{x \in \mathbb{Z}_p} \sum_{a \in A} \zeta^{jax^r}\right| \\
&\leqslant \frac{1}{r} \sum_{a \in A} \left|\sum_{x \in \mathbb{Z}_p} \zeta^{jax^r}\right| \\
&\leqslant \frac{1}{r} \sum_{a \in A} (r-1)\sqrt{p} = \frac{t(r-1)}{r}\sqrt{p} \\
&= O(\sqrt{p}),
\end{aligned} \tag{6.2}$$

since $t \leqslant r$, where we have used a well-known rth power character sum estimate in bounding $|\sum_x \zeta^{jax^r}|$ (e.g., see [BS66]). Note that in this case S has density $t/r + o(1)$.

We next exhibit a large (but more elementary) class of quasi-random sets. For a fixed integer $n > 1$, arbitrarily fix $X \subset \mathbb{Z}_n$ with $x := |X|$ satisfying $0 < x < n$. For $t > 1$, each $z \in \mathbb{Z}_{n^t}$ can be expressed uniquely as $z = \sum_{i=0}^{t-1} z_i n^i$, $0 \leqslant z_i < n$ (this is just the standard base n expansion of z). Define $S_t(X) \subset \mathbb{Z}_{n^t}$ by

$$S_t(X) := \{z \in \mathbb{Z}_{n^t} \mid \text{an odd number of } z_i \text{ belonging to } X\}.$$

PROPOSITION 2. *For all $j \neq 0$ in $\mathbb{Z}_{2^t}$, we have*

$$\frac{1}{n^t}\left|\sum_{z \in S_t(X)} \exp\frac{2\pi ijz}{n^t}\right| = o(1) \qquad as \quad t \to \infty. \tag{6.3}$$

This implies in particular that the sets $S_t(X)$ are quasi-random subsets of $\mathbb{Z}_{n^t}$. In general, $|S_t(X)| = (1+o(1))(n^t/2)$. We will only give the proof of (6.3) in the simplest case $n=2$, $X=\{1\}$, since the general case follows much the same lines but with somewhat more complicated notation. In this case, S_t consists of all $z \in \mathbb{Z}_{2^t}$ which have an *odd* number of 1's in their binary expansion (there are 2^{t-1} such z).

CLAIM. *For all $j \neq 0$ in $\mathbb{Z}_{2^t}$,*

$$\left|\sum_{z \in S_t} \exp\frac{2\pi ijz}{2^t}\right| \leqslant c(\sqrt{2+\sqrt{2}})^t \tag{6.4}$$

for an absolute constant c.

Proof. Let $w_m := \exp(2\pi i/2^m)$ and let $wt(z)$ denote the number of 1's in the binary expansion of z. For $j \in \mathbb{Z}_{2^m}$, define

$$\sum_m(j) := \sum_{\substack{z \in \mathbb{Z}_{2^m} \\ wt(z)\ \text{odd}}} w_m^{jz}.$$

Observe that

$$\sum_{z \in \mathbb{Z}_{2^m}} w_m^{jz} = \begin{cases} 0 & \text{if } j \not\equiv 0 \pmod{2^m}, \\ 2^m & \text{if } j \equiv 0 \pmod{2^m}. \end{cases} \tag{6.5}$$

Each $z \in \mathbb{Z}_{2^m}$ can be written uniquely as $z = x + 2y$ with $x \in \{0,1\}$, $y \in \mathbb{Z}_{2^{m-1}}$. Thus, we have the basic recurrence

$$\begin{aligned}
\sum_t(j) &= \sum_{z \in S_t} w_j^{jz} \\
&= \sum_{x+2y \in S_t} w_t^{j(x+2y)} \\
&= \sum_{\substack{x=0 \\ wt(y)\ \text{odd}}} w_t^{j(x+2y)} + \sum_{\substack{x=1 \\ wt(y)\ \text{even}}} w_t^{j(x+2y)} \\
&= \sum_{y \in S_{t-1}} w_t^{2jy} + w_t^j \sum_{y \in \mathbb{Z}_{2^{t-1}} \setminus S_{t-1}} w_t^{2jy} \\
&= \sum_{t-1}(j) + \begin{cases} w_t^j(-\sum_{t-1}(j)) & \text{if } j \not\equiv 0 \pmod{2^{t-1}} \\ w_t^j(2^{t-2}) & \text{if } j \equiv 0 \pmod{2^{t-1}},\ j \not\equiv 0 \pmod{2^t} \end{cases} \\
&= \begin{cases} (1-w_t^j)\sum_{t-1}(j) & \text{if } j \not\equiv 0 \pmod{2^{t-1}} \\ 0 & \text{if } j \equiv 0 \pmod{2^{t-1}},\ j \not\equiv 0 \pmod{2^t} \end{cases}
\end{aligned} \tag{6.6}$$

by (6.5). Iterating this argument, we obtain

$$\sum_t (j) = (1 - w_t^j)(1 - w_{t-1}^j) \sum_{t-2} (j) \qquad \text{if} \quad j \not\equiv 0 \pmod{2^{t-2}}$$

and 0 otherwise, $j \not\equiv 0 \pmod{2^t}$, etc. Continuing this process we find that for $j \not\equiv 0 \pmod{2^t}$,

$$\sum_t (j) = \begin{cases} -\prod_{k=2}^{t} (1 - w_k^j) & \text{if } j \text{ is odd,} \\ 0 & \text{if } j \text{ is even.} \end{cases} \tag{6.7}$$

Our next job is to estimate $|\prod_{k=2}^{t} (1 - w_k^j)|$. To begin, write $j = \sum_{i=0}^{t-1} j_i 2^i$, $j_i = 0, 1$, for a fixed odd $j \in \mathbb{Z}_{2^t}$ and define

$$j^{(m)} = \sum_{i=0}^{m-1} j_i 2^i.$$

Note that

$$w_m^j = \exp\left(\frac{2\pi i j}{2^m}\right) = w_m^{j^{(m)}}.$$

Focusing on the term $|1 - w_m^{j^{(m)}}|$, we want to consider the three initial "digits" $j_{m-1}\, j_{m-2}\, j_{m-3}$ of $j^{(m)}$. Easy geometrical computations show the following bounds on $|1 - w_{rn}^{j^{(m)}}|$, depending on $j_{m-1}\, j_{m-2}\, j_{m-3}$ (see Table I).

For example, if $j_{m-1}\, j_{m-2}\, j_{m-3} = 0\,0\,0$ then $j^{(m)} \leqslant \sum_{i=0}^{m-4} 1 \cdot 2^i < 2^{m-3}$. Thus,

$$|1 - w_m^j| < \left|1 - \exp\left(\frac{2\pi i}{8}\right)\right| = \sqrt{2 - \sqrt{2}}, \qquad \text{etc.}$$

TABLE I

j_{m-1}	j_{m-2}	j_{m-3}	Upper bound B on $\lvert 1 - w_m^{j^{(m)}} \rvert$
0	0	0	$\sqrt{2-\sqrt{2}}$
0	0	1	$\sqrt{2}$
0	1	0	$\sqrt{2+\sqrt{2}}$
0	1	1	2
1	0	0	2
1	0	1	$\sqrt{2+\sqrt{2}}$
1	1	0	$\sqrt{2}$
1	1	1	$\sqrt{2-\sqrt{2}}$

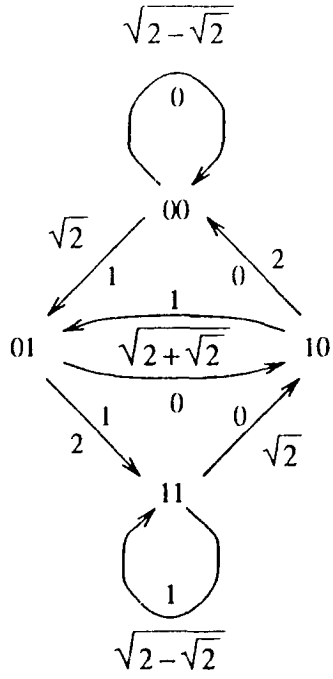

FIGURE 2

Finally, we construct the transition arc digraph G shown in Fig. 2 (cf. [KN81]). The interpretation of G is the following. Each edge $\alpha\beta \xrightarrow[B]{\gamma} \beta\gamma$ indicates the triple $\alpha\beta\gamma$ occurs as $j_{m-1}\, j_{m-2}\, j_{m-3}$ as the initial pair of digits go from $j_{m-1}\, j_{m-2} = \alpha\beta$ to $j_{m-2}\, j_{m-3} = \beta\gamma$. The bound B for $\alpha\beta\gamma$ is also shown in the edge. It is now simply a matter of finding the (simple) cycle C in G for which the $|C|$th root of the product of the corresponding edge bounds is as large as possible. This turns out to be the cycle $01 \to 10 \to 01$ which has (average) value $\sqrt{2+\sqrt{2}}$. Since we start with $j = j^{(t)}$ and walk for $t-2$ steps, the maximum possible value we can obtain is bounded by $c(\sqrt{2+\sqrt{2}})^t$ for some absolute constant c. This proves the claim. ∎

7. Concluding Remarks

In the preceding sections we have only managed to hint at the variety of properties of subsets of $\mathbb{Z}_n$ which are quasi-random. It would be of great interest to expand this list substantially. For example, Erdös [Er(x)] has suggested that the following sets S_n should be quasi-random. Call an

integer n "good" if it has at least $\log\log n$ prime factors. Define $S_n := \{m < n: m \text{ is good}\} \subset \mathbb{Z}_n$. No doubt other number-theoretic functions possessing a "normal order" would work as well (cf. [HW65]).

Of course, it is possible in principle to replace all occurrences of $o(1)$, etc., by explicit functions of n. Indeed, we hope to do this soon in a forthcoming paper. In this quantitative form, one could measure more explicitly the extent to which a specific set behaves like a random subset of $\mathbb{Z}_n$.

A natural direction one might pursue is the extension of this philosophy to other groups, e.g., finite abelian groups, permutation groups over finite fields, etc. Also it is natural to explore the possible links of these ideas to the well-studied subject of (infinite) pseudo-random sequences (e.g., see [Kn81]). There clearly remains much to be done.

REFERENCES

[BS66] Z. BOREVICH AND I. SHAFAREVICH, "Number Theory," Academic Press, New York, 1966.

[BT81] B. BOLLOBÁS AND A. THOMASON, Graphs which contain all small graphs, *European J. Combin.* **2** (1981), 13–15.

[CH81] F. R. K. CHUNG, A note on constructive methods for Ramsey numbers, *J. Graph Theory* **5** (1981), 109–113.

[Ch90] F. R. K. CHUNG, Quasi-random classes of hypergraphs, *Random Structures Algorithms* **1** (1990), 363–382.

[CG90] F. R. K. CHUNG AND R. L. GRAHAM, Quasi-random hypergraphs, *Random Structures Algorithms* **1** (1990), 105–124.

[CG91] F. R. K. CHUNG AND R. L. GRAHAM, Quasi-random tournaments, *J. Graph Theory* **15** (1991), 173–198.

[CG(b)] F. R. K. CHUNG AND R. L. GRAHAM, Maximum cuts and quasi-random graphs, to appear.

[CG90a] F. R. K. CHUNG AND R. L. GRAHAM, On graphs with missing prescribed induced subgraphs, *in* "A tribute to Paul Erdös" (A. Baker *et al.*, Eds.), pp. 111–120, Cambridge Univ. Press, 1990.

[CGW89] F. R. K. CHUNG, R. L. GRAHAM, AND R. M. WILSON, Quasi-random graphs, *Combinatorica* **9** (1989), 345–362.

[CT(a)] F. R. K. CHUNG AND P. TETALI, Communication complexity and quasi-randomness, preprint.

[Da79] P. J. DAVIS, "Circulant Matrices," Wiley, New York, 1979.

[Er(x)] P. ERDÖS, personal communication.

[ES82] P. ERDÖS AND V. T. SÓS, On Ramsey–Turán type theorems for hypergraphs, *Combinatorica* **2** (1982), 289–295.

[Fr77] P. FRANKL, A constructive lower bound for some Ramsey numbers, *Ars Combin.* **3** (1977), 297–302.

[Fr90] P. FRANKL, Intersection theorems and mod p rank of inclusion matrices, *J. Combin. Theory Ser. A* **54** (1990), 85–94.

[FG85] P. FRANKL AND R. L. GRAHAM, Intersection theorems for vector spaces, *European J. Combin.* **6** (1985), 183–187.

[FR89] P. FRANKL AND V. RÖDL, Some Ramsey–Turán type results for hypergraphs, *Combinatorica* **8** (1989), 323–332.

[FRW88] P. FRANKL, V. RÖDL, AND R. M. WILSON, The number of submatrices of given type in a Hadamard matrix and related results, *J. Combin. Theory Ser. B* **44** (1988), 317–328.

[Ga77] F. R. GANTMACHER, "The Theory of Matrices," Vol. 1, Chelsea, New York, 1977.

[GKP89] R. L. GRAHAM, D. E. KNUTH, AND O. PATASHNIK, "Concrete Mathematics," Addison–Wesley, Reading, MA, 1989.

[GS71] R. L. GRAHAM AND J. H. SPENCER, A constructive solution to a tournament problem, *Canad. Math. Bull.* **14** (1971), 45–48.

[HW65] G. H. HARDY AND E. M. WRIGHT, "The Theory of Numbers," Oxford Univ. Press, London, 1965.

[Ha89] J. HAVILAND, "Cliques and Independent Sets," Ph.D. thesis, Cambridge University, 1989.

[HT89] J. HAVILAND AND A. THOMASON, Pseudo-random hypergraphs, *Discrete Math.* **75** (1989), 255–278.

[IR82] K. IRELAND AND M. ROSEN, "A Classical Introduction to Modern Number Theory," Springer-Verlag, New York, 1982.

[Kr81] D. E. KNUTH, "The Art of Computer Programming. Vol. 2. Seminumerical Algorithms," 2nd ed., Addison–Wesley, Reading, MA, 1981.

[KN74] L. KUIPERS AND H. NIEDERREITER, "Uniform Distribution of Sequences," Wiley, New York, 1974.

[Rö86] V. RÖDL, On the universality of graphs with uniformly distributed edges, *Discrete Math.* **59** (1986), 125–134.

[Se77] J. P. SERRE, "Linear Representations of Finite Groups," Springer-Verlag, New York, 1977.

[SS91] M. SIMONOVITS AND V. T. SÓS, Szemerédi partitions and quasi-randomness, *Random Structures Algorithms* **2** (1991), 1–10.

[ST(a)] J. SPENCER AND P. TETALI, Quasi-random graphs with tolerance ε, preprint.

[Th87(a)] A. THOMASON, Random graphs, strongly regular graphs, and pseudo-random graphs, *in* "Survey in Combinatorics 1987" (C. Whitehead, Ed.), Lecture Notes in Math., Springer-Verlag, New York/Berlin, 1987.

[TH87(b)] A. THOMASON, Pseudo-random graphs, *in* "Proceedings, Random Graphs, Poznán, 1985" (M. Karónski, Ed.), Annals of Discrete Math., Vol. 33, pp. 307–331, North Holland, Amsterdam, 1987.

[Th89] A. THOMASON, Dense expanders and pseudo-random bipartite graphs, *Discrete Math.* **75** (1989), 381–386.

[Wi72] R. M. WILSON, Cyclotomy and difference families on abelian groups, *J. Number Theory* **4** (1972), 17–47.

[Wi74] R. M. WILSON, Constructions and uses of pairwise balanced designs, *in* "Combinatorics" (M. Hall, Jr., and J. H. van Lint, Eds.), Math. Centre Tracts, No. 55, pp. 18–41, Math. Centrum, Amsterdam, 1974.

[Wi90] R. M. WILSON, A diagonal form for the incidence matrix of t-subsets vs. k-subsets, *European J. Combin.* **11** (1990), 609–615.