ANNALS OF MATHEMATICS

Divergent square averages

By Zoltán Buczolich and R. Daniel Mauldin

SECOND SERIES, VOL. 171, NO. 3

May, 2010

ANMAAH

Annals of Mathematics, **171** (2010), 1479–1530

Divergent square averages

By ZOLTÁN BUCZOLICH and R. DANIEL MAULDIN

Abstract

In this paper we answer a question of J. Bourgain which was motivated by questions A. Bellow and H. Furstenberg. We show that the sequence $\{n^2\}_{n=1}^{\infty}$ is L^1-universally bad. This implies that it is not true that given a dynamical system (X, Σ, μ, T) and $f \in L^1(\mu)$, the ergodic means

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(T^{n^2}(x))$$

converge almost surely.

1. Introduction

Research related to almost everywhere convergence of ergodic averages along the squares was initiated by questions of A. Bellow (see [3]) and of H. Furstenberg [10]. Results of Bourgain [4], [5], [7] imply that given a dynamical system (X, Σ, μ, T) and $f \in L^p(\mu)$, for some $p > 1$, the ergodic means

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} f(T^{n^2}(x)) \tag{1}$$

converge almost surely. Bourgain also asked in [6], [7] whether this result is true for L^1-functions. In this paper we give a negative answer to this question.

Let us recall some concepts related to this problem.

Z.B.'s work was started during his visit at the Department of Mathematics of University of North Texas and later was supported by the Hungarian National Foundation for Scientific Research T049727 and K75242.

R.D.M. was supported in part by NSF grants DMS-0400481, 0700831 and as a van Fleck Visiting Researcher at Wesleyan University during 2005.

Definition 1. A sequence $\{n_k\}_{k=1}^{\infty}$ is L^1-*universally bad* if for all ergodic dynamical systems there is some $f \in L^1$ such that

$$\lim_{N\to\infty} \frac{1}{N} \sum_{k=1}^{N} f(T^{n_k} x)$$

fails to exist for all x in a set of positive measure.

By the Conze principle and the Banach principle of Sawyer (see [9], [16], or [17]), the sequence $\{n_k\}_{k=1}^{\infty}$ is L^1-universally bad if there is no constant $C < \infty$ such that for all systems (X, Σ, μ, T) and all $f \in L^1(\mu)$ we have the following weak $(1,1)$ inequality for all $t \in \mathbb{R}$:

$$\mu\left(\left\{x : \sup_{N\geq 1} \left|\frac{1}{N} \sum_{k=1}^{N} f(T^{n_k} x)\right| > t\right\}\right) \leq \frac{C}{t} \int |f| d\mu. \tag{2}$$

The main result of this paper is

THEOREM 1. *The sequence* $\{k^2\}_{k=1}^{\infty}$ *is* L^1-*universally bad.*

This theorem will be proved by showing that there is no constant C such that the weak $(1,1)$ inequality given in (2) holds.

This paper is a new and substantially modified version of our preprint from 2003. The proof in that preprint contained a gap but the methods of that paper lead to a solution of a counting problem raised by I. Assani (see [1] and [2]).

The paper is organized as follows. In Section 2 we develop the necessary ingredients we need concerning the asymptotic distribution of squares modulo q where q is the product of κ distinct primes. The specific technical property we need is given in Lemma 2. In Section 3 we develop the notion of a periodic rearrangement of a given periodic set. Lemma 3 states a property about the frequency squares hit such sets; we will need this later in our construction. Section 4 is the technical heart of the paper. For positive integers K, M and a periodic set Λ we define the notion of a $K-M$ family living on Λ. What we need for the proof of our main theorem is the existence of some specific families living on $\Lambda = \mathbb{R}$. The properties of these families are stated in Lemma 5. However, we need a double induction argument to show that such families exist. In Section 4.1, in Lemma 6 assuming $K-M$ families exist for all parameter values on $\mathbb{R}$, we show that they exist on periodic sets Λ. In Section 4.2 we turn to the proof that if $K-M$ families exist, then $(K+1)-M$ families exist as well, this induction on K is our outer inductive construction. In Sections 4.2.1 through 4.2.8 we carry out the first step of this induction, while in Sections 4.2.9 through 4.2.15 we show how this first step of the induction should be altered for $(K+1)-M$ families when $K > 0$. The proof of the existence of $(K+1)-M$ families involves an intricate inner inductive construction, the "leakage process", which is outlined in Section 4.2.1 and carried out in Sections 4.2.2 through 4.2.7. Once it has halted, it is shown in Section 4.2.8 how to adjust the functions so that the next stage of the outer induction holds. In Section 5, we give the proof of the main theorem. We construct a sequence of rational rotations T_p, functions f_p and numbers t_p which witness that there is no constant C satisfying (2).

To understand the heuristics behind our proof it might also be useful to look at [8].

If someone prefers to have a general overview of the main ideas of the paper before turning to the details here is a recommended quick tour: After reading the introduction read Definition 3. Then jump to Section 5 and read the statement of Theorem 8. Skip the proof of this theorem and read the details of the proof of Theorem 1 at the end of Section 5. Then continue with Section 2 and read it until (3). Jump to Definition 2 and Remark 1. Then read Section 4 starting at Definition 4 until the statements of Lemmas 5 and 6. From here jump to Section 4.2 and read it until the paragraph above 4.2.1. Continue with Lemma 2 and the paragraph above it. Read Remark 2. Then jump to Section 3 and read it until Lemma 3 is stated. Finally, read Section 4.2.1 until the paragraph containing (57).

Let us fix some notation. Given $f : \mathbb{R} \to \mathbb{R}$, periodic by p we put

$$\overline{\int} f = \frac{1}{p} \int_0^p f(x)dx.$$

Given a Lebesgue measurable set A, periodic by p we put

$$\overline{\lambda}(A) = \frac{1}{p}\lambda(A \cap [0, p)) = \lim_{N\to\infty} \frac{\lambda(A \cap [-N, N])}{2N}.$$

2. Number theory/quadratic residues

For each $q \in \mathbb{N}$ and $n \in \mathbb{Z}$ set $\varepsilon(n, q) = 1$ if n is congruent to a square modulo q, and let $\varepsilon(n, q) = 0$ if not. We denote by σ_q the number of squares modulo q. If p is an odd prime, then $\sigma_p = \frac{p+1}{2}$. If $q = p_1 \cdots p_\kappa$ where $p_1, \ldots, p_\kappa$ are distinct odd primes, then (by the fact that something is a square modulo q if and only if it is a square modulo each p_i plus by using the Chinese remainder theorem) $\sigma_q = \prod_{i=1}^{\kappa} \frac{p_i+1}{2}$. For elementary properties of quadratic residues see [11, pp. 67–69], or [14, Ch. 3]. We remark that though $0^2 = 0$, when talking about quadratic residues usually only those are considered which are not congruent to 0, but since $\varepsilon(n, q) = 1$ when n is congruent to 0 modulo q we will regard 0 a quadratic residue (or square) in this paper.

In Section 3 we will use the *Legendre symbol*. If τ is an odd prime the Legendre symbol $\left(\frac{n}{\tau}\right) = \left(\frac{n}{\tau}\right)_{\mathcal{L}}$ equals 0 if τ divides n, otherwise it equals $+1$ if

n is a square modulo τ and equals -1 if n is not a square modulo τ. To avoid notational confusion we will use the subscript $\mathscr{L}$ for the Legendre symbol. It is a character, that is, $\left(\frac{nm}{\tau}\right)_{\mathscr{L}} = \left(\frac{n}{\tau}\right)_{\mathscr{L}}\left(\frac{m}{\tau}\right)_{\mathscr{L}}$, and $1+\left(\frac{n}{\tau}\right)_{\mathscr{L}}$ equals the number of solutions $x \ mod \ \tau$ to the congruence $x^2 \equiv n \ mod \ \tau$.

Put $\Lambda_0(q) = \{n \in \mathbb{Z} : \varepsilon(n,q) = 1\}$, the set of integers which are quadratic residues modulo q. Clearly,

$$\#(\Lambda_0(q) \cap [0,q)) = \sigma_q > \frac{q}{2^\kappa}. \tag{3}$$

Next we discuss some results from [15] concerning the distribution of the squares modulo q. Given K, consider a fixed sequence $(\varepsilon_1,\dots,\varepsilon_K)$ of zeros and ones. Assume that $a_1,\dots,a_K$ are distinct integers modulo an odd prime p.

Set $\nu_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K) = \#\{n : 0 \le n < p,\ \varepsilon(n+a_i,p) = \varepsilon_i \text{ for } i = 1,\dots,K\}$, that is, $\nu_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K)$ counts the number of occurrences of $(\varepsilon_1,\dots,\varepsilon_K)$ in translated copies of $a_1,\dots,a_K$ modulo p. Then

$$\frac{p}{2^K} - K(3+\sqrt{p}) \le \nu_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K) \le \frac{p}{2^K} + K(3+\sqrt{p}).$$

The "probability" of the occurrence of $(\varepsilon_1,\dots,\varepsilon_K)$ in translated copies of $(a_1,\dots,a_K)$ is

$$\mathscr{P}_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K) = \frac{\nu_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K)}{p}$$

and by the above result if $(a_1,\dots,a_K)$ is fixed, then

$$\mathscr{P}_p(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K) \to \frac{1}{2^K} \text{ as the odd prime } p \to \infty. \tag{4}$$

Next we want to choose square free numbers $q = p_1 \cdots p_\kappa$, where $p_1,\dots,p_\kappa$ are distinct sufficiently large odd primes with good statistical properties.

A number n is a square modulo q if and only if it is a square modulo each of the primes $p_1,\dots,p_\kappa$. By (4), given $a_1,\dots,a_K$ and keeping κ, fixed as $\min\{p_1,\dots\ \dots,p_\kappa\} \to \infty$ we have

$$\mathscr{P}_q(\varepsilon_1,\dots,\varepsilon_K;a_1,\dots,a_K) \to \left(\frac{1}{2^\kappa}\right)^{\sum_{i=1}^K \varepsilon_i} \left(1-\frac{1}{2^\kappa}\right)^{K-\sum_{i=1}^K \varepsilon_i}; \tag{5}$$

that is, statistically squares modulo q look like outcomes of independent Bernoulli trials with probabilities $\frac{1}{2^\kappa}$ and $\left(1-\frac{1}{2^\kappa}\right)$. Without going into technical details of this fact from number theory, we just give an outline of a proof by induction on κ. For $\kappa = 1$, (5) follows from (4). Suppose $\kappa > 1$ and (5) holds for $\kappa - 1$. Set $q_0 = p_1 \cdots p_{\kappa-1}$. For any possible choice of $\varepsilon' = (\varepsilon'_1,\dots,\varepsilon'_K)$ and $\varepsilon'' = (\varepsilon''_1,\dots,\varepsilon''_K)$, set $W(\varepsilon',\varepsilon'') = \{n : 0 \le n < q,\ \varepsilon(n+a_i,q_0) = \varepsilon'_i \text{ and } \varepsilon(n+a_i,p_\kappa) = \varepsilon''_i \text{ for } i = 1,\dots,K\}$, $W_0(\varepsilon') = \{n : 0 \le n < q_0,\ \varepsilon(n+a_i,q_0) = \varepsilon'_i \text{ for } i = 1,\dots,K\}$, and $W_\kappa(\varepsilon'') = \{n : 0 \le n < p_\kappa,\ \varepsilon(n + a_i, p_\kappa) = \varepsilon''_i$ for $i = 1, \dots, K\}$. Observe that for any n the numbers $n + jq_0$, $j = 0, \dots, p_\kappa - 1$ hit each residue class modulo p_κ exactly once, and $\varepsilon(n + jq_0 + a_i, q_0) = \varepsilon(n + a_i, q_0)$ for all i. Using this one can see that $W_0(\varepsilon')$ and $W_\kappa(\varepsilon'')$ are independent in the sense that $\#W(\varepsilon', \varepsilon'') = \#W_0(\varepsilon')\#W_\kappa(\varepsilon'')$. For $\varepsilon = (\varepsilon_1, \dots, \varepsilon_K)$, set $G(\varepsilon) = \{n : 0 \le n < q$, $\varepsilon(n+a_i, q) = \varepsilon_i$ for $i = 1, \dots, K\}$. Then $\#G(\varepsilon) = \sum \#W(\varepsilon', \varepsilon'')$, where the sum is taken over all pairs $(\varepsilon', \varepsilon'')$ whose coordinatewise product is ε. Taking the limit as $\min p_1, \dots, p_\kappa$ goes to infinity of $\#G(\varepsilon)/q$, using (4) for the limit of $\#W_\kappa(\varepsilon'')/p_\kappa$ and (5) for the limit of $\#W_0(\varepsilon')/q_0$, and noting that the only thing that matters in these limiting probabilities is the number of 1's in the sequence, we have after setting $m = \sum_{i=1}^K \varepsilon_i$, that the limiting value is

$$\frac{1}{2^K} \sum_{i=0}^{K-m} \binom{K-m}{i} \left(\frac{1}{2^{\kappa-1}}\right)^m \left(1 - \frac{1}{2^{\kappa-1}}\right)^i = (\frac{1}{2^\kappa})^m \left(1 - \frac{1}{2^\kappa}\right)^{K-m},$$

which is what we wanted.

Consider an infinite sequence of pairwise independent random variables $X_i : Y \to \{0, 1\}$ with $P(X_i(\omega) = 1) = \frac{1}{2^\kappa}$, $P(X_i(\omega) = 0) = 1 - \frac{1}{2^\kappa}$. Then $E(X_i(\omega)) = \frac{1}{2^\kappa}$. By the law of large numbers if $\rho > 0$ and $K \to \infty$, then

$$P\left(\left|\frac{1}{K}\sum_{i=1}^K X_i(\omega) - \frac{1}{2^\kappa}\right| \ge \rho\right) \to 0.$$

Given $\rho, \epsilon_1 > 0$ if K is large enough, then

$$P\left(\left|\frac{1}{K}\sum_{i=1}^K X_i(\omega) - \frac{1}{2^\kappa}\right| \ge \rho\right) < \epsilon_1.$$

For odd primes $p_1 < p_2 < \cdots < p_\kappa$ put $q = p_1 \cdots p_\kappa$. Given distinct integers $a_1, \dots, a_K$ consider $X_i(n) = \varepsilon(n + a_i, q)$. By (5) as $p_1 \to \infty$ the variables $X_i(n)$ approximate independent random variables with Bernoulli distribution $\frac{1}{2^\kappa}$, $\left(1 - \frac{1}{2^\kappa}\right)$. Hence, given a sufficiently large K if p_1 is sufficiently large then

$$\frac{\#\{n \in [0, q) : \left|\frac{1}{K}\sum_{i=1}^K \varepsilon(n + a_i, q) - \frac{1}{2^\kappa}\right| \ge \rho\}}{q} < \epsilon_1.$$

In particular, we have

$$\#\left\{n \in [0, q) : \sum_{i=1}^K \varepsilon(n + a_i, q) \ge \frac{K}{2^\kappa} + K\rho\right\} < \epsilon_1 q. \tag{6}$$

For later arguments we now introduce some parameters. We will need a suitably small "leakage constant" $\gamma \in (0, 1)$ of the form $\gamma = 2^{-c_\gamma}$ where $c_\gamma \in \mathbb{N}$. Then we work with $\kappa > c_\gamma$. Furthermore we use small constants $\rho, \rho_1 > 0$. For large K_1 we have

(7) $$K_2 \stackrel{\text{def}}{=} \lceil (1+\rho_1 2^\kappa)\gamma K_1 \rceil < (1+\rho_1)(1+\rho_1 2^\kappa)\gamma K_1 \text{ and } \gamma 2^\kappa / K_1 < \epsilon_1.$$

Thus for a large K_1 we can choose p_1' such that

(8) $$p_1' > \max\{K_1 + \gamma 2^\kappa, K_1/\epsilon_1\}$$

and, in addition if $p_1 > p_1'$ we have for any $q = p_1 \cdots p_\kappa$, $p_1 < \cdots < p_\kappa$,

(9) $$\#\left\{ n \in [0,q) : \left| \frac{1}{K_1} \sum_{i=1}^{K_1} \varepsilon(n+i,q) - \frac{1}{2^\kappa} \right| \geq \rho \right\} < \epsilon_1 q.$$

Also, we can choose $p_1'' \geq p_1'$ such that if $p_1 > p_1''$ then given any integers $a_1, \ldots, a_{K_2}$ so that the difference of any two of them is less than p_1' we also have, after a simple change of notation in (6)

(10) $$\#\left\{ n \in [0,q) : \sum_{i=1}^{K_2} \varepsilon(-(n+a_i),q) \geq \frac{K_2}{2^\kappa} + K_2 \rho_1 \right\} < \epsilon_1 q,$$

the negative sign in the first argument of $\varepsilon(\cdot, q)$ is due to technical reasons in later arguments; it is clear that if n takes all possible values modulo q then so does $-n$.

Let $n_1 \in [0, \infty)$ be the first number for which

$$\mathfrak{D}(K_1, n_1, q) \stackrel{\text{def}}{=} \left| \frac{1}{K_1} \sum_{i=1}^{K_1} \varepsilon(n_1+i,q) - \frac{1}{2^\kappa} \right| < \rho.$$

Next choose the least $n_2 \geq n_1 + K_1$ such that $\mathfrak{D}(K_1, n_2, q) < \rho$.

Continue and set $\mathcal{J} = \{j \in \mathbb{N} : 0 \leq n_j < q\}$. If $n' \in [0,q) \setminus \cup_{j \in \mathcal{J}} [n_j, n_j + K_1)$, then $\mathfrak{D}(K_1, n', q) \geq \rho$ holds.

Hence, by (9)

(11) $$\#\left\{ n \in [0,q) : n \notin \bigcup_{j \in \mathcal{J}} [n_j, n_j + K_1) \right\} < \epsilon_1 q.$$

If $j \in \mathcal{J}$, then by the definition of $\varepsilon(n,q)$

(12) $$K_1 \left(\frac{1}{2^\kappa} - \rho \right) < \#\Big(\Lambda_0(q) \cap [n_j + 1, n_j + K_1] \Big) < K_1 \left(\frac{1}{2^\kappa} + \rho \right),$$

so that the number of quadratic residues modulo q in the interval $[n_j + 1, n_j + K_1]$ is approximately $K_1/2^\kappa$.

Definition 2. Set $\Lambda_\gamma(q) = -\Lambda_0(q) + \{j \in \mathbb{Z} : 0 \leq j < \gamma 2^\kappa\}$, $\overline{\Lambda}_\gamma(q) = \Lambda_\gamma(q) + [0,1) = -\Lambda_0(q) + \{x : 0 \leq x < \gamma 2^\kappa\}$. For ease of notation in the sequel if we have a fixed γ and we do not want to emphasize the dependence on γ we will write $\Lambda(q)$ and $\overline{\Lambda}(q)$, instead of $\Lambda_\gamma(q)$ and $\overline{\Lambda}_\gamma(q)$, respectively. (To make it easier to memorize our notation for these Λ type sets it will be useful to keep in mind that the sets Λ without the bars will be subsets of $\mathbb{Z}$ and the sets $\overline{\Lambda} \subset \mathbb{R}$ will be obtained from the corresponding Λ sets by adding $[0, 1)$.)

Remark 1. Here are some "heuristic" comments related to the above definition.

If $\Lambda_0(q)$ equaled $\{k \cdot 2^\kappa : k \in \mathbb{Z}\}$, then $\overline{\lambda}(\overline{\Lambda}(q))$ would equal γ.

Next suppose that $\Lambda_0(q)$ is the set of quadratic residues. If the intervals making up $\overline{\Lambda}_\gamma(q))$ were disjoint, then $\overline{\lambda}(\overline{\Lambda}_\gamma(q))$ would be $\gamma \prod_{i=1}^{\kappa} \frac{p_i+1}{p_i}$, somewhat larger than γ. However, by results in [13] for a fixed γ as κ goes to ∞, the normalized gaps between consecutive elements of $\Lambda_0(q)$ converge to an exponential distribution. We will make explicit use of this fact in Lemma 7. Since the normalizing factor is σ_q, the number of squares modulo q approximately equals $q/2^\kappa$ and the average value of the spacing between elements of $\Lambda_0(q)$ is very close to 2^κ. For each κ sufficiently large if p_1 is sufficiently large, for a certain percentage of different elements $i, i' \in \Lambda_0(q)$ the intervals $[i, i + \gamma 2^\kappa)$ and $[i', i' + \gamma 2^\kappa)$ will overlap. Under these conditions $\overline{\lambda}(\overline{\Lambda}(q))$ will be less than γ, but the smaller γ is, the closer $\overline{\lambda}(\overline{\Lambda}(q))/\gamma$ is to 1 for large q's. We will take advantage of this property particularly when we fix a leakage constant.

By Remark 1, $\#((\mathbb{Z} \cap [0, q)) \setminus \Lambda(q))$ is a little larger than $(1-\gamma)\#(\mathbb{Z} \cap [0, q))$ for large κ and p_1.

Suppose $\rho > 0$ is given. If a q-periodic set $A \subset \mathbb{Z}$ is "not sufficiently ρ-independent" from $\Lambda(q)$ it may happen that

$$\#((A \setminus \Lambda(Q)) \cap [0, q)) < (1-\rho)(1-\gamma)\#(A \cap [0, q)). \tag{13}$$

In the next lemma we consider translated copies of $\Lambda_0(q)$. We show that for q's with large prime factors there is only a small portion of n's when $A_n = n + \Lambda_0(q)$ satisfies (13).

LEMMA 2. *Given a positive integer κ and $\epsilon, \rho > 0$ there exists p_1'' such that if the odd primes satisfy $p_1'' < p_1 < \cdots < p_\kappa$ and $q = p_1 \cdots p_\kappa$, then*

$$\begin{aligned} \#\Big\{n \in [0, q) : \#\Big(\big((n + \Lambda_0(q)) \setminus \Lambda(q)\big) \cap [0, q)\Big) \\ < (1-\rho)(1-\gamma)\#\Big(\Lambda_0(q) \cap [0, q)\Big)\Big\} < \epsilon q. \end{aligned} \tag{14}$$

Remark 2. The heuristics behind (14) are the following. The number of $n \in [0, q)$ for which $n \in \Lambda(q)$ is a little less than γq, due to "overlaps". This means that the number of those n's for which $n \notin \Lambda(q)$ is a little larger than $(1-\gamma)q$. Now one can examine what happens when we look at translated copies of $\Lambda_0(q)$.

Formula (14) says that for "most" translated copies of $\Lambda_0(q)$ we cannot have much less than $(1-\gamma)\#(\Lambda_0(q)\cap[0,q))$ elements of $n+\Lambda_0(q)$ outside $\Lambda(q)$.

Before beginning the proof of Lemma 2 we choose $\rho_0>0$ such that

$$\left(1-\frac{1}{(1-\rho_0)^2}\gamma\right)>(1-\rho)(1-\gamma). \tag{15}$$

Recall from number theory that if p_1'' is sufficiently large then we have

$$(1-\rho_0)\frac{q}{2^\kappa}<\#(\Lambda_0(q)\cap[0,q))=\sigma_q<\frac{1}{(1-\rho_0)}\frac{q}{2^\kappa}. \tag{16}$$

Proof. We can assume that $\epsilon<1$. Take $0<\epsilon_1<\epsilon^2/32$ and then choose K_1, p_1' and p_1'' as above. By (8) and $q>p_1''\geq p_1'$ we have $q>K_1/\epsilon_1$ and by (11)

$$\#\left\{n\in[0,q):n\notin\bigcup_{j\in\mathcal{J}}[n_j,n_j+K_1)\right\}<\epsilon_1 q \tag{17}$$

for a suitable index set $\mathcal{J}$, defined above, and for each $j\in\mathcal{J}$ we have $\mathcal{D}(K_1,n_j,q)<\rho_1$ for a suitable $\rho_1>0$. This means that

$$K_1\left(\frac{1}{2^\kappa}-\rho_1\right)<\#(\Lambda_0(q)\cap[n_j+1,n_j+K_1])<K_1\left(\frac{1}{2^\kappa}+\rho_1\right). \tag{18}$$

By Definition 2 for $n\in[0,q)$ we have $n+n'\in\Lambda(q)=\Lambda_\gamma(q)$ if $n+n'-i\in-\Lambda_0(q)$ holds for an $i=0,\dots,\gamma 2^\kappa-1$. Set $\Lambda_0^j(q)=\Lambda_0(q)\cap[n_j+1,n_j+K_1]$ and

$$\Lambda^j(q)=-\left(\bigcup_{i=0}^{\gamma 2^\kappa-1}(\Lambda_0^j(q)-i)\right)$$

for each $j\in\mathcal{J}$. Using the definition of K_2 in (7), and (18) choose distinct numbers $a_{i',j}$, $i'=1,\dots,K_2$, so that

$$-\Lambda^j(q)=\bigcup_{i=0}^{\gamma 2^\kappa-1}\Lambda_0^j(q)-i\subseteq A_j\stackrel{\text{def}}{=}\bigcup_{i'=1}^{K_2}\{a_{i',j}\}\subset[n_j-\gamma 2^\kappa,n_j+K_1]. \tag{19}$$

Clearly, by the choice of p_1' in (8) the difference of any two of the $a_{i',j}$'s is less than p_1'. By (19)

$$(n+\Lambda_0(q))\cap\Lambda^j(q)\subset(n+\Lambda_0(q))\cap(-A_j).$$

Observe that there exists $n'\in\Lambda_0(q)$ such that $n+n'\in-A_j$ if and only if there exists i' such that $n+n'=-a_{i',j}$, that is, $n+a_{i',j}=-n'\in-\Lambda_0(q)$.

Recall that $n+a_{i',j}\in-\Lambda_0(q)$ if and only if $\varepsilon(-(n+a_{i',j}),q)=1$. Set $N_j=\{n\in[0,q):\sum_{i'=1}^{K_2}\varepsilon(-(n+a_{i',j}),q)\geq K_2(\frac{1}{2^\kappa}+\rho_1)\}$. If $n\notin N_j$, $n\in[0,q)$

then

$$\#\left((n+\Lambda_0(q))\cap\Lambda^j(q)\right)<K_2\left(\frac{1}{2^\kappa}+\rho_1\right). \tag{20}$$

By (10)

$$\#N_j<\epsilon_1 q. \tag{21}$$

Here we remark that (10) can be used so that we have (21) for all $j\in\mathcal{J}$. Indeed, assume $A\subset[-\gamma 2^\kappa,K_1]$ and $A+n_j=A_j$, then

$$N_j=N_A\overset{\text{def}}{=}\left\{n\in[0,q):\sum_{a\in A}\varepsilon(-(n+a),q)\geq K_2\left(\frac{1}{2^\kappa}+\rho_1\right)\right\}.$$

There are $2^{\gamma 2^\kappa+K_1+1}$ subsets of $[-\gamma 2^\kappa,K_1]$. So, we can choose p_1'' before (10) so that we have $\#N_A<\epsilon_1 q$ for all subsets A of $[-\gamma 2^\kappa,K_1]$.

If $n\notin N_j$, $n\in[0,q)$, then by (7) and (20)

$$\begin{aligned}\#((n+\Lambda_0(q))\cap\Lambda^j(q))&<K_2\left(\frac{1}{2^\kappa}+\rho_1\right)\\&<(1+\rho_1)(1+\rho_1 2^\kappa)\gamma K_1\left(\frac{1}{2^\kappa}+\rho_1\right).\end{aligned} \tag{22}$$

On the other hand, by (17)

$$\frac{q-\epsilon_1 q}{K_1}\leq\#\mathcal{J}<\frac{q}{K_1}+1. \tag{23}$$

For $0\leq n<q$ set $\mathcal{J}(n)=\{j\in\mathcal{J}:n\notin N_j\}$.

Consider an n such that

$$\#\mathcal{J}(n)>q\frac{1-\epsilon_1}{K_1}(1-\sqrt{\epsilon_1}). \tag{24}$$

Later we show that for most n's this inequality holds.

Observe that if $x\in[-(n_j+K_1)+\gamma 2^\kappa-1,-n_j-1]\cap\Lambda(q)$ then there exists $i\in\{0,\dots,\gamma 2^\kappa-1\}$ such that $x-i\in-\Lambda_0(q)$ and $x-i\in[-(n_j+K_1),-n_j-1]$, that is, $x-i\in-\Lambda_0^j(q)$ and hence $x\in\Lambda^j(q)$. Therefore, $[-(n_j+K_1)+\gamma 2^\kappa-1,-n_j-1]\cap\Lambda(q)\subset\Lambda^j(q)$.

We want to estimate

$$\#\left(((n+\Lambda_0(q))\setminus\Lambda(q))\cap[0,q)\right)=\#\left(((n+\Lambda_0(q))\setminus\Lambda(q))\cap(-q,0]\right).$$

By (22) for any $j\in\mathcal{J}(n)$

$$\begin{aligned}&\#((n+\Lambda_0(q))\cap\Lambda(q)\cap[-(n_j+K_1)+\gamma 2^\kappa-1,-n_j-1)\\&\qquad<(1+\rho_1)(1+\rho_1 2^\kappa)\gamma K_1\left(\frac{1}{2^\kappa}+\rho_1\right).\end{aligned} \tag{25}$$

Put

$$T_n = \left\{ t \in \mathbb{Z} : t \in (-q, 0] \setminus \bigcup_{j \in \mathcal{J}(n)} [-(n_j + K_1) + \gamma 2^{\kappa} - 1, -n_j - 1] \right\}.$$

It is clear that

(26)

$$\begin{aligned} &(n + \Lambda_0(q)) \cap \Lambda(q) \cap (-q, 0] \\ &\quad \subset T_n \cup \bigcup_{j \in \mathcal{J}(n)} (n + \Lambda_0(q)) \cap \Lambda(q) \cap [-(n_j + K_1) + \gamma 2^{\kappa} - 1, -n_j - 1]. \end{aligned}$$

We need to estimate $\# T_n$. Since the intervals $[-(n_j + K_1), -n_j - 1]$ are disjoint and, with the possible exception of the one with the largest index, are subsets of $(-q, 0]$ we have by using (7) and (24)

$$\begin{aligned} \# T_n &< q - \#\mathcal{J}(n)(K_1 - \gamma 2^{\kappa}) < q - \#\mathcal{J}(n)(1 - \epsilon_1) K_1 \\ &< q - q \frac{(1-\epsilon_1)^2}{K_1} (1 - \sqrt{\epsilon_1}) K_1 = q(1 - (1-\epsilon_1)^2 (1 - \sqrt{\epsilon_1})) < q c_1(\epsilon_1), \end{aligned}$$

where $c_1(\epsilon_1) \to 0$ as $\epsilon_1 \to 0$. Now we use this, (25) and (26) to estimate

$$\begin{aligned} &\#\Big((n + \Lambda_0(q)) \cap \Lambda(q) \cap (-q, 0] \Big) \\ &\quad < \#\mathcal{J}(n) \cdot (1 + \rho_1)(1 + \rho_1 2^{\kappa}) \gamma K_1 \left(\frac{1}{2^{\kappa}} + \rho_1 \right) + q c_1(\epsilon_1) \end{aligned}$$

(using (23))

$$\begin{aligned} &< \left(\frac{q}{K_1} + 1 \right) (1 + \rho_1)(1 + \rho_1 2^{\kappa}) \gamma K_1 \left(\frac{1}{2^{\kappa}} + \rho_1 \right) + q c_1(\epsilon_1) \\ &= \left(1 + \frac{K_1}{q} \right) (1 + \rho_1)(1 + \rho_1 2^{\kappa})^2 \gamma q \frac{1}{2^{\kappa}} + q c_1(\epsilon_1) \end{aligned}$$

(using (8) and $q > p_1' > K_1/\epsilon_1$)

$$\begin{aligned} &< (1 + \epsilon_1)(1 + \rho_1)(1 + \rho_1 2^{\kappa})^2 \gamma q \frac{1}{2^{\kappa}} + q c_1(\epsilon_1) \\ &= \left((1 + \epsilon_1)(1 + \rho_1)(1 + \rho_1 2^{\kappa})^2 + \frac{2^{\kappa}}{\gamma} c_1(\epsilon_1) \right) \gamma q \frac{1}{2^{\kappa}} = c_2(\epsilon_1, \rho_1) \gamma q \frac{1}{2^{\kappa}}, \end{aligned}$$

where $c_2(\epsilon_1, \rho_1) \to 1$ as $\epsilon_1, \rho_1 \to 0$.

We can choose $\epsilon_1, \rho_1 > 0$ so that

$$c_2(\epsilon_1, \rho_1) < \frac{1}{(1 - \rho_0)}.$$

This by (16) implies

$$c_2(\epsilon_1,\rho_1)\gamma q\frac{1}{2^\kappa}<\frac{1}{(1-\rho_0)^2}\gamma\#(\Lambda_0(q)\cap[0,q)).$$

By (15) we obtain

$$\begin{aligned}(27)\quad \#\Big(((n+\Lambda_0(q))\setminus\Lambda(q))\cap[0,q)\Big)&>\#(\Lambda_0(q)\cap[0,q))(1-\frac{1}{(1-\rho_0)^2}\gamma)\\ &>\#(\Lambda_0(q)\cap[0,q))(1-\rho)(1-\gamma).\end{aligned}$$

To prove (14) we need to show that there are sufficiently many n's which satisfy the above inequality.

Let b be the number of n's for which

$$\#\mathcal{J}(n)\le q\frac{1-\epsilon_1}{K_1}(1-\sqrt{\epsilon_1}). \tag{28}$$

If we can show that $b<\epsilon q$, then we have finished the proof of Lemma 2 since if (24) holds for an n then we have (27). If n satisfies (28) then by the definition of $\mathcal{J}(n)$ from (23) we infer that $n\in N_j$ for at least $\sqrt{\epsilon_1}\frac{1-\epsilon_1}{K_1}q$ many j's. Hence, using (21) and (23)

$$b\sqrt{\epsilon_1}\frac{1-\epsilon_1}{K_1}q\le\sum_{j\in\mathcal{J}}\#N_j\le\epsilon_1 q(\frac{q}{K_1}+1)<\frac{2\epsilon_1 q^2}{K_1}$$

which implies

$$b\le\frac{2\sqrt{\epsilon_1}}{1-\epsilon_1}q<\epsilon q. \qquad\square$$

3. **Periodic rearrangements**

We need a lemma concerning the fact that one can make a periodic perturbation of certain given periodic sets so that averages of the characteristic function of the perturbed set taken along squares is close to the average measure of the original set.

Assume $F\subset\mathbb{R}$ is periodic by $\tau'\in\mathbb{N}$ and if $x\in F$ then $[\lfloor x\rfloor,\lfloor x\rfloor+1)\subset F$. Given a natural number $\tau>\tau'$, the τ*-periodic rearrangement* of F is denoted by F^τ and it is periodic by τ, and $F^\tau\cap[0,\tau)=[0,\lfloor\tau/\tau'\rfloor\cdot\tau')\cap F$.

For the proof of the next lemma we recall that by the Pólya-Vinogradov Theorem (see for example page 324 of [12]) for any $n\in\mathbb{Z}$, $l\in\mathbb{N}$ and odd prime τ, we have $\sum_{j=n}^{n+l-1}\left(\frac{j}{\tau}\right)_{\mathcal{L}}\le 6\sqrt{\tau}\log\tau$.

LEMMA 3. *Suppose $\tau\in\mathbb{N}$, $F\subset\mathbb{R}$ periodic by τ' and $\rho>0$ are given. There exists M_ρ such that if $\tau>M_\rho$ is a prime number then for any $n\in\mathbb{N}$ and $x\in\mathbb{R}$, if*

$\tau|m$, then

$$\frac{1}{m}\sum_{k=n}^{n+m-1}\chi_{F^{\tau}}(x+k^2)\geq(1-\rho)\overline{\lambda}(F). \tag{29}$$

Proof. For each $a\in\{1,\dots,\tau'\}$, let $F_a=\cup_{n\equiv a \pmod{\tau'}}[n,n+1)$. Since F is the disjoint union of finitely many of the sets F_a, it suffices to prove the lemma for some fixed F_a. Also, note that it is enough to show that there is some M_ρ such that if $\tau>M_\rho$ is a prime number, then for any $n\in\mathbb{N}$ and $x\in\mathbb{R}$,

$$\frac{1}{\tau}\sum_{k=n}^{n+\tau-1}\chi_{F_a^{\tau}}(x+k^2)\geq(1-\rho)\overline{\lambda}(F_a)=\frac{1-\rho}{\tau'}. \tag{30}$$

Put $l=\lfloor\tau/\tau'\rfloor$.

Note $\chi_{F_a^{\tau}}(x+k^2)=1$ for an integer x if and only if there is some $j\in\{0,\dots,l-1\}$ such that $x+k^2\equiv a+j\tau' \pmod{\tau}$.

Thus, using the Legendre symbol $\left(\frac{k}{n}\right)_{\mathcal{L}}$, we have

$$\begin{aligned}
&\frac{1}{\tau}\#\{k\in\{0,\dots,\tau-1\}:k^2\equiv a+j\tau'-x,\ \pmod{\tau}\text{ for a }j\in\{0,\dots,l-1\}\}\\
&\quad=\frac{1}{\tau}\sum_{j=0}^{l-1}\#\{k\in\{0,\dots,\tau-1\}:k^2\equiv a+j\tau'-x,\ \pmod{\tau}\}\\
&\quad=\frac{1}{\tau}\sum_{j=0}^{l-1}\left(1+\left(\frac{a+j\tau'-x}{\tau}\right)_{\mathcal{L}}\right)=\frac{l}{\tau}+\frac{1}{\tau}\sum_{j=0}^{l-1}\left(\frac{a+j\tau'-x}{\tau}\right)_{\mathcal{L}}\\
&\quad=\frac{\lfloor\tau/\tau'\rfloor}{\tau}+\frac{1}{\tau}\sum_{j=0}^{l-1}\left(\frac{a+j\tau'-x}{\tau}\right)_{\mathcal{L}}.
\end{aligned}$$

Now as $\tau\to\infty$, $\frac{\lfloor\tau/\tau'\rfloor}{\tau}\to\frac{1}{\tau'}$. Setting $S=\sum_{j=0}^{l-1}\left(\frac{a+j\tau'-x}{\tau}\right)_{\mathcal{L}}$ we only need to show $S/\tau\to 0$, as $\tau\to\infty$.

We argue this as follows. Since τ' is a prime with $\tau'<\tau$, choose b such that $b\tau'\equiv a-x,\ \pmod{\tau}$ and set $\tau^*=(\tau')^{-1},\ \pmod{\tau}$ so that $b\equiv(a-x)\cdot\tau^*,\ \pmod{\tau}$. Since the Legendre symbol is a character,

$$\left(\frac{(a+j\tau'-x)\cdot\tau^*}{\tau}\right)_{\mathcal{L}}=\left(\frac{a+j\tau'-x}{\tau}\right)_{\mathcal{L}}\cdot\left(\frac{\tau^*}{\tau}\right)_{\mathcal{L}}.$$

Also, we have $|\left(\frac{\tau^*}{\tau}\right)_{\mathcal{L}}| = 1$. Since

$$\left(\frac{(a+j\tau'-x)\cdot\tau^*}{\tau}\right)_{\mathcal{L}} = \left(\frac{(a-x)\tau^*+j\tau'\tau^*}{\tau}\right)_{\mathcal{L}} = \left(\frac{b+j}{\tau}\right)_{\mathcal{L}},$$

we have by the Pólya-Vinogradov inequality

$$|S| = \left|\sum_{j=0}^{l-1}\left(\frac{b+j}{\tau}\right)_{\mathcal{L}}\right| \leq 6\sqrt{\tau}\log\tau \text{ and } \frac{|S|}{\tau} \to 0 \text{ as } \tau\to\infty.$$

This completes the proof of Lemma 3. □

4. $K-M$ families

Definition 3. For a positive integer M we say that a periodic function or a "random variable", $X:\mathbb{R}\to\mathbb{R}$ is *conditionally* M*−0.99 distributed* on the set Λ, which is periodic by the same period, if $X(x)\in\{0, 0.99, 0.99\cdot\frac{1}{2},\dots,0.99\cdot 2^{-M+1}\}$, and $\overline{\lambda}(\{x\in\Lambda : X(x)=0.99\cdot 2^{-l}\})=0.99\cdot 2^{-M+l-1}\overline{\lambda}(\Lambda)$ for $l=0,\dots,M-1$. (We regard $\mathbb{R}$ as being periodic by 1 with $\overline{\lambda}(\mathbb{R})=1$ and if $\Lambda=\mathbb{R}$ then we just simply say that X is $M-0.99$-distributed.) By an obvious adjustment this definition will also be used for random variables $\overline{X}$ defined on $[0,1)$ equipped with the Lebesgue measure λ. If we have two "random variables" X_1 and X_2 both conditionally $M-0.99$ distributed on Λ then they are called pairwise independent (on Λ) if for any $y_1, y_2\in\mathbb{R}$

(31)
$$\overline{\lambda}\{x\in\Lambda : X_1(x)=y_1 \text{ and } X_2(x)=y_2\}\overline{\lambda}(\Lambda)$$
$$= \overline{\lambda}(\{x\in\Lambda : X_1(x)=y_1\})\overline{\lambda}(\{x\in\Lambda : X_2(x)=y_2\})$$

or, equivalently,

$$\overline{\lambda}\{x\in\Lambda : X_1(x)=y_1 \text{ and } X_2(x)=y_2\}/\overline{\lambda}(\Lambda)$$
$$= (\overline{\lambda}(\{x\in\Lambda : X_1(x)=y_1\})/\overline{\lambda}(\Lambda))(\overline{\lambda}(\{x\in\Lambda : X_2(x)=y_2\})/\overline{\lambda}(\Lambda)).$$

If we say that X_1 and X_2 are pairwise independent, without specifying Λ then we mean $\Lambda=\mathbb{R}$.

We will use the following simple properties. Assume Λ_1 and Λ_2 are two disjoint sets with a common period. If X_1 and X_2 are conditionally $M-0.99$ distributed on Λ_1 and on Λ_2, then X_1 (and similarly X_2) is conditionally $M-0.99$ distributed on $\Lambda_1\cup\Lambda_2$. If, in addition X_1 and X_2 are pairwise independent on each Λ_1 and Λ_2, then X_1 and X_2 are pairwise independent on $\Lambda_1\cup\Lambda_2$. We note the last property depends on X_1 and X_2 having the *same distribution* on Λ_1 and Λ_2.

Similar properties hold if we have finitely many functions $X_1, \dots, X_K$ with the same conditional distribution.

For our argument a wide range of independent, identically distributed uniformly bounded "random variables" with expectations bounded from below by constant times $M2^{-M}$ could be used. However, as the remark above shows we need identically distributed random variables and out of the many possible choices we picked the $M-0.99$ distributed ones. For a motivation for this choice see [8].

We say that $X : \mathbb{R} \to \mathbb{R}$ is $M-0.99$ super distributed if

$$X(x) \in \{0, 0.99, 0.99 \cdot 2^{-1}, \dots, 0.99 \cdot 2^{-M+1}\}, \tag{32}$$

and

$$\overline{\lambda}(\{x \in \mathbb{R} : X(x) = 0.99 \cdot 2^{-l}\}) \geq 0.99 \cdot 2^{-M+l-1} \text{ for } l = 0, \dots, M-1.$$

We need the following lemma:

LEMMA 4. *Suppose* $\tau \in \mathbb{N}$, $X_1, \dots, X_K : \mathbb{R} \to [0, \infty)$ *are* $M-0.99$ *distributed,* τ *periodic and* X'_{K+1} *is* $M-0.99$ *super distributed* τ *periodic and* X'_{K+1} *is pairwise independent from* X_h *for all* $h = 1, \dots, k$. *Then we can choose* $0 \leq X_{K+1} \leq X'_{K+1}$ *such that* X_{K+1} *is* $M-0.99$ *distributed and pairwise independent from* X_h *for all* $h = 1, \dots, k$.

Proof. Set

$$\Theta'_{K+1,l} \stackrel{\text{def}}{=} \{x \in \mathbb{R} : X'_{K+1}(x) = 0.99 \cdot 2^{-l}\}.$$

Then $\overline{\lambda}(\Theta'_{K+1,l}) \geq 0.99 \cdot 2^{-M+l-1}$ and

$$1 \geq c_l \stackrel{\text{def}}{=} \frac{0.99 \cdot 2^{-M+l-1}}{\overline{\lambda}(\Theta'_{K+1,l})}.$$

We also set $\mathcal{S}_K = \{0, 0.99, \dots, 0.99 \cdot 2^{-M+1}\}^K$ and for $(y_1, \dots, y_K) \in \mathcal{S}_K$ set

$$\Theta'_{K+1,l}(y_1, \dots, y_K) \stackrel{\text{def}}{=} \{x \in \Theta'_{K+1,l} : X_h(x) = y_h,\ h = 1, \dots, K\}.$$

Clearly, $\Theta'_{K+1,l}(y_1, \dots, y_K)$ is τ periodic and for $(y_1, \dots, y_K) \neq (y'_1, \dots, y'_K) \in \mathcal{S}_K$ the sets $\Theta'_{K+1,l}(y_1, \dots, y_K)$ and $\Theta'_{K+1,l}(y'_1, \dots, y'_K)$ are disjoint. For all $(y_1, \dots, y_K) \in \mathcal{S}_K$ choose a Borel measurable

$$\Theta_{K+1,l}(y_1, \dots, y_K) \subset \Theta'_{K+1,l}(y_1, \dots, y_K)$$

such that

$$\overline{\lambda}(\Theta_{K+1,l}(y_1, \dots, y_K)) = c_l \overline{\lambda}(\Theta'_{K+1,l}(y_1, \dots, y_K))$$

and $\Theta_{K+1,l}(y_1, \dots, y_K)$ is periodic by τ.

For $x \in \Theta_{K+1,l}(y_1, \dots, y_K)$ set $X_{K+1}(x) = X'_{K+1}(x) = 0.99 \cdot 2^{-l}$ and for $x \in \Theta'_{K+1,l}(y_1, \dots, y_K) \setminus \Theta_{K+1,l}(y_1, \dots, y_K)$ set $X_{K+1}(x) = 0$. Do this for all

$(y_1, \dots, y_K) \in \mathcal{S}_K$ and for all $l = 0, \dots, M-1$. Finally, for those x's for which $X'_{K+1}(x) = 0$ set $X_{K+1}(x) = 0$. Then $0 \le X_{K+1} \le X'_{K+1}$.

Suppose $l \in \{0, \dots, M-1\}$ is fixed. Then

$$\overline{\lambda}(\{x : X_{K+1}(x) = 0.99 \cdot 2^{-l}\}) = \sum_{(y_1,\dots,y_K)\in\mathcal{S}_K} \overline{\lambda}(\Theta_{K+1,l}(y_1, \dots, y_K))$$

$$= \sum_{(y_1,\dots,y_K)\in\mathcal{S}_K} c_l \overline{\lambda}(\Theta'_{K+1,l}(y_1, \dots, y_K)) = c_l \overline{\lambda}(\Theta'_{K+1,l}) = 0.99 \cdot 2^{-M+l-1}.$$

This and (32) also implies that

$$\overline{\lambda}(\{x : X_{K+1}(x) = 0\}) = 1 - \sum_{l=0}^{M-1} 0.99 \cdot 2^{-M+l-1}. \tag{33}$$

Suppose $\overline{y}_h \in \{0, 0.99, 0.99 \cdot 2^{-1}, \dots, 0.99 \cdot 2^{-M+1}\}$ is fixed and denote by $\mathcal{S}_{K,\overline{y}_h}$ the set of those $(y_1, \dots, y_K) \in \mathcal{S}_K$ for which $y_h = \overline{y}_h$. Then by the pairwise independence of X_h and X'_{K+1} on $\mathbb{R}$ we have

$$\begin{aligned}
\overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X'_{K+1}(x) = 0.99 \cdot 2^{-l}\}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\})\overline{\lambda}(\{x : X'_{K+1}(x) = 0.99 \cdot 2^{-l}\}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\})\overline{\lambda}(\Theta'_{K+1,l}).
\end{aligned} \tag{34}$$

On the other hand,

$$\begin{aligned}
\sum_{(y_1,\dots,y_K)\in\mathcal{S}_{K,\overline{y}_h}} \overline{\lambda}(\Theta'_{K+1,l}(y_1, \dots, y_K)) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X'_{K+1}(x) = 0.99 \cdot 2^{-l}\}).
\end{aligned} \tag{35}$$

Since

$$\begin{aligned}
c_l \sum_{(y_1,\dots,y_K)\in\mathcal{S}_{K,\overline{y}_h}} \overline{\lambda}(\Theta'_{K+1,l}(y_1, \dots, y_K)) \\
&= \sum_{(y_1,\dots,y_K)\in\mathcal{S}_{K,\overline{y}_h}} \overline{\lambda}(\Theta_{K+1,l}(y_1, \dots, y_K)) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X_{K+1}(x) = 0.99 \cdot 2^{-l}\}),
\end{aligned}$$

if we multiply (34) and (35) by c_l we obtain

$$\begin{aligned}
\overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X_{K+1}(x) = 0.99 \cdot 2^{-l}\}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\}) \cdot c_l \cdot \overline{\lambda}(\Theta'_{K+1,l}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\}) \cdot 0.99 \cdot 2^{-M+l-1} \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\})\overline{\lambda}(\{x : X_{K+1}(x) = 0.99 \cdot 2^{-l}\}).
\end{aligned}$$

By (32) and (33) we also have

$$
\begin{aligned}
&\overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X_{K+1}(x) = 0\}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\}) - \sum_{l=0}^{M-1} \overline{\lambda}(\{x : X_h(x) = \overline{y}_h \text{ and } X_{K+1}(x) = 0.99 \cdot 2^{-l}\}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\})(1 - \sum_{l=0}^{M-1} 0.99 \cdot 2^{-M+l-1}) \\
&= \overline{\lambda}(\{x : X_h(x) = \overline{y}_h\})\overline{\lambda}(\{x : X_{K+1}(x) = 0\}).
\end{aligned}
$$

This completes the proof of the fact that X_{K+1} is pairwise independent from X_h for all $h = 1, \ldots, K$. $\square$

Definition 4. We say that a set $\mathcal{P} \subset \mathbb{N}$ has *sufficiently large complement* if there are infinitely many primes relatively prime to any number in $\mathcal{P}$.

Sometimes we need to work with the "real" squares modulo q:

Definition 5. Assume $q = p_1 \cdots p_\kappa$, where $p_1 < \cdots < p_\kappa$ are odd primes. Set

$$\Lambda_0'(q) = \{n \in \Lambda_0(q) : p_j \not| n, \text{ for all } j = 1, \ldots, \kappa\}.$$

If $n \in \Lambda_0'(q)$, then there are 2^κ many solutions of $x^2 \equiv n \ mod \ q$, also observe that for fixed κ

$$\text{if } p_1 \to \infty, \text{ then } \frac{\#(\Lambda_0(q) \cap [0, q))}{\#(\Lambda_0'(q) \cap [0, q))} \to 1. \tag{36}$$

Given $\gamma \in (0, 1)$ we also put

$$
\begin{aligned}
\Lambda_\gamma'(q) &= -\Lambda_0'(q) + \{j \in \mathbb{Z} : 0 \le j < \gamma 2^\kappa\}, \\
\overline{\Lambda}_\gamma'(q) &= \Lambda_\gamma'(q) + [0, 1) = -\Lambda_0'(q) + \{x : 0 \le x < \gamma 2^\kappa\}.
\end{aligned}
$$

In the sequel often if γ is fixed we will suppress the dependence on γ by writing $\Lambda'(q)$ and $\overline{\Lambda}'(q)$ instead of $\Lambda_\gamma'(q)$ and $\overline{\Lambda}_\gamma'(q)$, respectively. To help to memorize our notation of these sets, "Λ'" means that the set "Λ" is built as "Λ" but instead of Λ_0 we use Λ_0' in our construction. We keep our earlier convention as well and hence "$\overline{\Lambda}'$" is the set obtained from "Λ'" by adding $[0, 1)$.

Definition 6. Suppose $K, M \in \mathbb{N}$, $\Lambda \subset \mathbb{R}$ is periodic by $\widetilde{q}$. There is a parameter γ' associated to Λ. (If $\Lambda = \mathbb{R}$ then $\widetilde{q} = \gamma' = 1$. Otherwise one should think of $\Lambda = \overline{\Lambda}_{\gamma'}'(\widetilde{q})$ and γ' is the parameter used in the definition of Λ.) In the sequel we assume that $\mathcal{P} \subset \mathbb{N}$ has sufficiently large complement. A *$K - M$ family living on* Λ with input parameters $\delta > 0$, Ω, $\Gamma > 1$, $A \in \mathbb{N}$, $\mathcal{P}$ with output objects τ, f_h, X_h $(h = 1, \ldots, K)$; E_δ, $\omega(x)$, $\alpha(x)$ and $\tau(x)$ is a system satisfying:

(i) There exist a period τ, functions $f_h : \mathbb{R} \to [0, \infty)$, pairwise independent, conditionally M−0.99-distributed on Λ "random" variables $X_h : \mathbb{R} \to \mathbb{R}$, for $h = 1, \ldots, K$, and a set E_δ such that all these objects are periodic by τ where τ is an integer multiple of $\widetilde{q}$.

(ii) We have $\overline{\lambda}(E_\delta) < \delta$. For all $x \notin E_\delta$, there exist $\omega(x) > \alpha(x) > A$, $\tau(x) < \tau$ such that $\omega^2(x) < \tau$, $\frac{\omega(x)}{\alpha(x)} > \Omega \cdot \tau(x)$; moreover if $\alpha(x) \le n < n + m \le \omega(x)$ and $\tau(x)|m$, then for all $h = 1, \ldots, K$,

$$\frac{1}{m} \sum_{k=n}^{n+m-1} f_h(x + k^2) > X_h(x). \tag{37}$$

(iii) For all $p \in \mathcal{P}$, $(\tau(x), p) = 1$, $(\tau, p) = 1$.

(iv) For all $x \in \Lambda \setminus E_\delta$, for all $h \in \{1, \ldots, K\}$

$$f_h(x + j + \tau(x)) = f_h(x + j) \tag{38}$$

whenever $\alpha^2(x) \le j < j + \tau(x) \le \omega^2(x)$.

(v) Finally, for $h = 1, \ldots, K$

$$\frac{1}{\tau} \int_0^\tau f_h = \overline{\int} f_h < \Gamma \cdot \gamma' \cdot 2^{-M+1}. \tag{39}$$

Remark 3. The input parameters in the above definition should be regarded as something given in advance while the output objects are defined and constructed later. The most important property is (37), while the numerous other technical properties are needed in order to verify by mathematical induction the existence of $K - M$ families.

If x is not in the exceptional set E_δ, then (37) says that the average of f_h taken along the squares of a run of integers staying in the window $[\alpha(x), \omega(x)]$ dominates $X_h(x)$, provided that the length of the run is a multiple of $\tau(x)$. In (38) we claim that these functions appear to be periodic in the window $[\alpha^2(x), \beta^2(x)]$, that is, when squares stay in the window $[\alpha(x), \beta(x)]$.

LEMMA 5. *Let* $M \in \mathbb{N}$, $\Lambda = \mathbb{R}$ (*this implies* $\widetilde{q} = \gamma' = 1$). *Then for each positive integer* K *and parameters* $\delta > 0$, $\Omega, \Gamma > 1$, $A \in \mathbb{N}$, *and* $\mathcal{P} \subset \mathbb{N}$ *such that* $\mathcal{P}$ *has sufficiently large complement there exist a* $K - M$ *family living on* $\mathbb{R}$ *with these parameters.*

4.1. *Putting* $K - M$ *families on quadratic residue classes.* The proof of Lemma 5 is quite involved. It will be done by induction on K. We will build a $(K + 1) - M$ family for a given set of input parameters, provided we know the existence of $K - M$ families for all possible input parameters. To carry out this induction step we need to verify that a generalized version of Lemma 5 holds.

So we assume that $K-M$ families on $\mathbb{R}$ exist for a fixed $K\in\mathbb{N}$ for all possible parameter values.

We will use the following lemma about "*putting a $K-M$-family on a residue class*". We assume that $\overline{\mathcal{P}}$ is a set of natural numbers with sufficiently large complement and we have a number $\widetilde{q}$ such that

$$(\widetilde{q},p)=1 \text{ for all } p\in\overline{\mathcal{P}},\ \widetilde{q}=p_{0,1}\cdots p_{0,\kappa}, \tag{40}$$

and $p_{0,1}<\cdots<p_{0,\kappa}$ are odd primes.

We also assume that a constant $\gamma=2^{-c_\gamma}$, the so called "leakage constant" is given with $c_\gamma\in\mathbb{N}$ and $\kappa>c_\gamma$. This γ is used in the definition of $\overline{\Lambda}'(\widetilde{q})=\overline{\Lambda}'_\gamma(\widetilde{q})$.

LEMMA 6. *Let $M\in\mathbb{N}$ be given and suppose for some $K\in\mathbb{N}$ that $K-M$ families exist on $\mathbb{R}$ for all possible parameter values. Suppose that $\overline{\mathcal{P}}$, $\widetilde{q}$ and the parameter γ associated to $\overline{\Lambda}'(\widetilde{q})$ satisfy the above assumptions. In addition, let $\delta>0$, $\Omega,\Gamma>1$, and $A\in\mathbb{N}$ be given. Then for the above input parameters there exists a $K-M$ family living on $\overline{\Lambda}'(\widetilde{q})$ with output objects $\overline{\tau}$, $\overline{f_h}$, $\overline{X}_h$ $(h=1,\dots,K)$; $\overline{E}_\delta$, $\overline{\omega}(x)$, $\overline{\alpha}(x)$ and $\overline{\tau}(x)$. Moreover, $\overline{\tau}=\tau\widetilde{q}$ with a suitable $\tau\in\mathbb{N}$ and if $\overline{\Xi}(\widetilde{q})=\cup_{j\in\mathbb{Z}}[j\widetilde{q},j\widetilde{q}+\gamma 2^\kappa)$ then $\overline{f_h}(x)=0$ for $x\notin\overline{\Xi}(\widetilde{q})$ and $h=1,\dots,K$.*

Proof. Using $\mathcal{P}=\overline{\mathcal{P}}\cup\{\widetilde{q}\}$, choose a $K-M$ family living on $\mathbb{R}$ with input parameters δ, $\Omega'=\Omega\widetilde{q}$, Γ, A. This $K-M$ family provides us with τ, f_h, X_h, E_δ, $\omega(x)$, $\alpha(x)$, and $\tau(x)$, satisfying (i)–(v) of Definition 6. Especially,

$$\text{for all } p\in\overline{\mathcal{P}}\cup\{\widetilde{q}\} \text{ we have } (\tau(x),p)=1 \text{ and } (\tau,p)=1. \tag{41}$$

We construct a new K-system, marked by overlines, which lives on $\overline{\Lambda}'(\widetilde{q})$ and is periodic by $\overline{\tau}=\tau\widetilde{q}$.

Set $\overline{f_h}(x)=f_h(x)\widetilde{q}/2^\kappa$ if $x\in\overline{\Xi}(\widetilde{q})=\cup_{j\in\mathbb{Z}}[j\widetilde{q},j\widetilde{q}+\gamma 2^\kappa)$, otherwise put $\overline{f_h}(x)=0$. Then $\overline{f_h}$ is periodic by $\tau\widetilde{q}$.

Next we define $\overline{X}_h(x)$ so that $\overline{X}_h(x)=X_h(x)$ for $x\in\overline{\Lambda}'(\widetilde{q})$, and otherwise let $\overline{X}_h(x)=0$. Clearly, $\overline{X}_h$ is periodic by $\tau\widetilde{q}$ and is supported on $\overline{\Lambda}'(\widetilde{q})$.

Next we check the distribution of $\overline{X}_h(x)|_{\overline{\Lambda}'(\widetilde{q})}$. We know that $X_h(x+\tau)=X_h(x)$. From (41), $(\tau,\widetilde{q})=1$ and thus the numbers $j\tau$, $j=0,\dots,\widetilde{q}-1$ cover all residue classes modulo $\widetilde{q}$. Now we can compute

$$\begin{aligned}
\overline{\lambda}(\{x\in\overline{\Lambda}'(\widetilde{q}):\overline{X}_h(x)&=0.99\cdot 2^{-l}\})\\
&=\overline{\lambda}(\{x\in\mathbb{R}:\overline{X}_h(x)=0.99\cdot 2^{-l}\})\\
&=\frac{1}{\tau\widetilde{q}}\lambda(\{x\in[0,\tau\widetilde{q}):\overline{X}_h(x)=0.99\cdot 2^{-l}\})\\
&=\frac{1}{\tau\widetilde{q}}\sum_{j=0}^{\widetilde{q}-1}\lambda(\{x\in[j\tau,(j+1)\tau):\overline{X}_h(x)=0.99\cdot 2^{-l}\})
\end{aligned}$$

$$= \frac{1}{\tau\widetilde{q}} \sum_{j=0}^{\widetilde{q}-1} \lambda(\{x \in [0,\tau) : \overline{X}_h(x + j\tau) = 0.99 \cdot 2^{-l}\})$$
$$= \frac{1}{\tau\widetilde{q}} \#(\Lambda'(\widetilde{q}) \cap [0, \widetilde{q})) \cdot \lambda(\{x \in [0,\tau) : X_h(x) = 0.99 \cdot 2^{-l}\})$$

(using that $\#(\Lambda'(\widetilde{q}) \cap [0, \widetilde{q}))/\widetilde{q} = \overline{\lambda}(\overline{\Lambda}'(\widetilde{q})))$

$$= \overline{\lambda}(\overline{\Lambda}'(\widetilde{q})) \cdot \frac{1}{\tau} \lambda(\{x \in [0,\tau) : X_h(x) = 0.99 \cdot 2^{-l}\})$$
$$= \overline{\lambda}(\overline{\Lambda}'(\widetilde{q})) \cdot \overline{\lambda}(\{x \in \mathbb{R} : X_h(x) = 0.99 \cdot 2^{-l}\}) = \overline{\lambda}(\overline{\Lambda}'(\widetilde{q})) \cdot 0.99 \cdot 2^{-M+l-1}.$$

Thus the "conditional distribution" of $\overline{X}_h$ on $\overline{\Lambda}'(\widetilde{q})$ is M–0.99.

Set $\Upsilon = \{0, 0.99, 0.99 \cdot 2^{-1}, \dots, 0.99 \cdot 2^{-M+1}\}$ and $\Upsilon_+ = \Upsilon \setminus \{0\}$. Next we show that the functions $\overline{X}_h$ are pairwise independent on $\overline{\Lambda}'(\widetilde{q})$. Suppose $h_1 \neq h_2$. First assume $y_1, y_2 \in \Upsilon_+$. Then the above argument shows

$$\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_j}(x) = y_j\}) = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_j}(x) = y_j\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})) \tag{42}$$

for $j = 1, 2$. A similar argument shows

$$\begin{aligned} &\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = y_1 \text{ and } \overline{X}_{h_2}(x) = y_2\}) \\ &\quad = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_1}(x) = y_1 \text{ and } X_{h_2}(x) = y_2\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})). \end{aligned} \tag{43}$$

The range of $\overline{X}_{h_j}$ and X_{h_j} equals $\Upsilon = \Upsilon_+ \cup \{0\}$ and (42) holds for all $y_j \in \Upsilon_+$. Therefore,

$$\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_j}(x) = 0\}) = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_j}(x) = 0\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})) \tag{44}$$

should also hold for $j = 1, 2$.

Recalling that X_{h_j} are $M-0.99$ distributed and pairwise independent on $\mathbb{R}$, using for a fixed $y_2 \in \Upsilon_+$, (43) for all $y_1 \in \Upsilon_+$, and using (42) with $j = 2$ one can deduce

$$\begin{aligned} &\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = 0 \text{ and } \overline{X}_{h_2}(x) = y_2\}) \\ &\quad = \overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_2}(x) = y_2\}) \\ &\qquad - \overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) \in \Upsilon_+ \text{ and } \overline{X}_{h_2}(x) = y_2\}) \\ &\quad = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_1}(x) = 0 \text{ and } X_{h_2}(x) = y_2\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})). \end{aligned} \tag{45}$$

Similarly, one can see that for any $y_1 \in \Upsilon_+$

$$\begin{aligned} &\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = y_1 \text{ and } \overline{X}_{h_1}(x) = 0\}) \\ &\quad = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_1}(x) = y_1 \text{ and } X_{h_2}(x) = 0\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})). \end{aligned} \tag{46}$$

Recalling that X_{h_2} is $M-0.99$-distributed on $\mathbb{R}$ and using (45) for all $y_2 \in \Upsilon_+$ and (44) with $j=1$ one can see that

$$\begin{aligned}(47)\quad \overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = 0 \text{ and } \overline{X}_{h_2}(x) = 0\}) \\ = \overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = 0\}) \\ -\overline{\lambda}(\{x \in \overline{\Lambda}'(\widetilde{q}) : \overline{X}_{h_1}(x) = 0 \text{ and } \overline{X}_{h_2}(x) \in \Upsilon_+\}) \\ = \overline{\lambda}(\{x \in \mathbb{R} : X_{h_1}(x) = 0 \text{ and } X_{h_2}(x) = 0\})\overline{\lambda}(\overline{\Lambda}'(\widetilde{q})).\end{aligned}$$

Since X_{h_1} and X_{h_2} are pairwise independent and $M-0.99$-distributed on $\mathbb{R}$, from (42)–(47) it follows that $\overline{X}_{h_1}$ and $\overline{X}_{h_2}$ are pairwise independent on $\overline{\Lambda}'(\widetilde{q})$.

Put $\overline{E}_\delta = E_\delta$. Clearly, $\overline{E}_\delta$ is periodic by $\overline{\tau}$ and this completes the proof of property (i) in the definition of a $K-M$ family.

It is clear that $\overline{\lambda}(\overline{E}_\delta) = \overline{\lambda}(E_\delta) < \delta$. For all $x \notin \overline{E}_\delta$, $h \in \{1, \dots, K\}$, let $\overline{\alpha}(x) = \alpha(x)$, $\overline{\omega}(x) = \omega(x)$, $\overline{\tau}(x) = \widetilde{q}\tau(x)$, then we have $\frac{\overline{\omega}(x)}{\overline{\alpha}(x)} > \Omega'\tau(x) = \Omega\widetilde{q}\tau(x) = \Omega\overline{\tau}(x)$.

Now we verify (37) for $\overline{f}_h$ and $\overline{X}_h$. Assume $x \in \overline{\Lambda}'(\widetilde{q}) \setminus \overline{E}_\delta$, $\overline{\alpha}(x) = \alpha(x) \le n < n+m \le \omega(x) = \overline{\omega}(x)$, $\overline{\tau}(x) = \tau(x)\widetilde{q}|m$. In fact, it is enough to consider the case when $\tau(x)\widetilde{q} = m = \overline{\tau}(x)$. We claim that for any $h = 1, \dots, K$ we have

$$\frac{1}{m}\sum_{k=n}^{n+m-1} f_h(x+k^2) \le \frac{1}{m}\sum_{k=n}^{n+m-1} \overline{f}_h(x+k^2),$$

then we will apply (37) for f_h, and X_h.

Since $\tau(x)\widetilde{q} = m$ and $x \in \overline{\Lambda}'(\widetilde{q}) \setminus \overline{E}_\delta$ implies $x \notin E_\delta$, using (38) several times we obtain

$$\begin{aligned}\frac{1}{m}\sum_{k=n}^{n+m-1} f_h(x+k^2) &= \frac{1}{m}\sum_{k'=n}^{n+\tau(x)-1}\sum_{j=0}^{\widetilde{q}-1} f_h(x+(k'+j\tau(x))^2) \\ &= \frac{1}{m}\sum_{k'=n}^{n+\tau(x)-1} \widetilde{q} f_h(x+k'^2).\end{aligned}$$

From $x \in \overline{\Lambda}'(\widetilde{q})$, it follows that there exists k_0 such that

$$x \in -k_0^2 + [i_{k_0}\widetilde{q}, i_{k_0}\widetilde{q} + \gamma 2^\kappa);$$

that is, $x + k_0^2 \in [i_{k_0}\widetilde{q}, i_{k_0}\widetilde{q} + \gamma 2^\kappa)$ for an $i_{k_0} \in \mathbb{Z}$, and $k_0^2 \in \Lambda_0'(\widetilde{q})$. Recall that there are 2^κ many solutions of $x^2 \equiv k_0^2$ modulo $\widetilde{q}$.

Since $(\tau(x), \widetilde{q}) = 1$ for a fixed k', the set $k' + j\tau(x)$ forms a complete residue system modulo $\widetilde{q}$ as j runs from 0 to $\widetilde{q}-1$, hence there are at least 2^κ many $j_{k',l}$'s $l = 1, \dots, 2^\kappa$ with $(k' + j_{k',l}\tau(x))^2 \equiv k_0^2$ modulo $\widetilde{q}$, where k_0 is defined above.

Recalling that $x \in \overline{\Lambda}'(\widetilde{q}) \setminus \overline{E}_\delta$, for any $k' = n, \dots, n+\tau(x)-1$, we have

$$\sum_{j=0}^{\widetilde{q}-1} \overline{f}_h(x+(k'+j\tau(x))^2) \geq \sum_{l=1}^{2^\kappa} \overline{f}_h(x+(k'+j_{k',l}\tau(x))^2)$$
$$= \sum_{l=1}^{2^\kappa} f_h(x+(k'+j_{k',l}\tau(x))^2)\frac{\widetilde{q}}{2^\kappa} \geq 2^\kappa f_h(x+k'^2)\frac{\widetilde{q}}{2^\kappa}.$$

Therefore,

$$\frac{1}{m}\sum_{k=n}^{n+m-1} \overline{f}_h(x+k^2) = \frac{1}{m}\sum_{k'=n}^{n+\tau(x)-1}\sum_{j=0}^{\widetilde{q}-1} \overline{f}_h(x+(k'+j\tau(x))^2)$$

applying (37) for f_h and X_h

$$\geq \frac{1}{m}\sum_{k'=n}^{n+\tau(x)-1} \widetilde{q} f_h(x+k'^2) = \frac{1}{m}\sum_{k=n}^{n+m-1} f_h(x+k^2) \geq X_h(x) \geq \overline{X}_h(x).$$

This proves (ii) for $x \in \overline{\Lambda}'(\widetilde{q}) \setminus \overline{E}_\delta$. Since $\overline{X}_h(x) = 0$ for $x \in \mathbb{R} \setminus (\overline{\Lambda}'(\widetilde{q}) \cup \overline{E}_\delta)$ for these x's (37) holds obviously for $\overline{f}_h$ and $\overline{X}_h$.

Using (41) and $(\widetilde{q}, p) = 1$ for all $p \in \overline{\mathcal{P}}$ we have $(\overline{\tau}(x), p) = (\widetilde{q}\tau(x), p) = 1$ and $(\tau\widetilde{q}, p) = (\overline{\tau}, p) = 1$ for all $p \in \overline{\mathcal{P}}$. This proves (iii).

To verify (iv), suppose $x \in \overline{\Lambda}'(\widetilde{q}) \setminus \overline{E}_\delta$, $h \in \{1, \dots, K\}$ and $\alpha^2(x) = \overline{\alpha}^2(x) \leq j < j + \widetilde{q}\tau(x) \leq \overline{\omega}^2(x) = \omega^2(x)$.

If $x + j \in \overline{\Xi}(\widetilde{q})$, then

$$\overline{f}_h(x+j) = f_h(x+j)\widetilde{q}/2^\kappa = f_h(x+j+\tau(x))\widetilde{q}/2^\kappa$$
$$= \cdots = f_h(x+j+\widetilde{q}\tau(x))\widetilde{q}/2^\kappa = \overline{f}_h(x+j+\widetilde{q}\tau(x)) \tag{48}$$

when $\alpha^2(x) = \overline{\alpha}^2(x) \leq j < j + \widetilde{q}\tau(x) \leq \overline{\omega}^2(x) = \omega^2(x)$.

If $x + j \notin \overline{\Xi}(\widetilde{q})$, then $\overline{f}_h(x+j) = 0 = \overline{f}_h(x+j+\widetilde{q}\tau(x))$. This verifies (iv).

Next we prove (v):

$$\frac{1}{\tau\widetilde{q}}\int_0^{\tau\widetilde{q}} \overline{f}_h = \overline{\int} \overline{f}_h \leq \Gamma \cdot \gamma \cdot 2^{-M+1}. \tag{49}$$

Indeed,

$$\frac{1}{\tau\widetilde{q}}\sum_{j=0}^{\widetilde{q}-1}\int_0^\tau \overline{f}_h(x+j\tau)dx = \frac{1}{\tau}\int_0^\tau \frac{1}{\widetilde{q}}\sum_{j=0}^{\widetilde{q}-1} \overline{f}_h(x+j\tau)dx = (*).$$

To continue this computation recall that from $(\tau, \widetilde{q}) = 1$ it follows that $\lfloor x \rfloor + j\tau$ hits each residue class modulo $\widetilde{q}$ once as j varies from 0 to $\widetilde{q}-1$ and $f_h(x+j\tau) = f_h(x)$

for all j. Thus, recalling that γ' associated to $\Lambda = \mathbb{R}$ equals 1 and using (v) for f_h

$$(*) = \frac{1}{\tau}\int_0^\tau \frac{1}{\widetilde{q}} f_h(x)\frac{\widetilde{q}}{2^\kappa}\gamma 2^\kappa dx = \frac{1}{\tau}\gamma\int_0^\tau f_h(x)dx \leq \Gamma\gamma 2^{-M+1}.$$

This proves (49). □

4.2. *Proof of Lemma 5.* Let a positive integer M be given together with input parameters $\delta > 0, \Omega, \Gamma < 1, A \in \mathbb{N}$ and $\mathcal{P} \subset \mathbb{N}$ with sufficiently large complement. To show the existence of a $(K+1) - M$ family living on $\mathbb{R}$, we need to fix several constants for the induction argument.

To begin with we will use the following Lemma 7 to choose a "leakage constant" which will remain fixed during the inductive construction of a $(K+1) - M$ family from $K - M$ families. This lemma is a more exact expression of the ideas given in Remark 1.

Considering the sets $\overline{\Lambda}'_\gamma(q)$, a direct calculation shows:

$$\overline{\lambda}(\overline{\Lambda}'_\gamma(q)) < \gamma \text{ and } \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'_\gamma(q)) > 1 - \gamma. \tag{50}$$

However, the closer γ to 0, the smaller the percentage of "loss due to overlaps". To obtain estimates from the opposite sides we will use Lemma 7.

LEMMA 7. *For each $0 < \gamma < 1/7$, one can choose constants $C_\gamma > 1 > \widetilde{C}_\gamma > 0$, $\kappa_\gamma \in \mathbb{N}$, such that for each $\kappa > \kappa_\gamma$ there exists $p_{\gamma,\kappa}$ for which if $p_{\gamma,\kappa} < p_1 < \cdots < p_\kappa$ and $q = p_1 \cdots p_\kappa$, then*

$$C_\gamma > \frac{\gamma}{\overline{\lambda}(\overline{\Lambda}'_\gamma(q))} \quad \textit{and} \quad \widetilde{C}_\gamma\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'_\gamma(q)) < 1 - \gamma - \gamma^2. \tag{51}$$

In fact, we can choose

$$C_\gamma = \frac{1}{1 - 7\gamma} \textit{ and } \widetilde{C}_\gamma = \frac{1 - \gamma - \gamma^2}{1 - \gamma + 7\gamma^2}.$$

Therefore, $C_\gamma \to 1$ and $\widetilde{C}_\gamma \to 1$ as $\gamma \to 0+$.

We remark that in (51) the second order term in $(1 - \gamma - \gamma^2)$ appears for technical reasons. It is clear that $(1 - \gamma - \gamma^2)/(1 - \gamma) \to 1$ as $\gamma \to 0+$.

Proof. We use the fact that the limiting distribution of the gaps between squares is continuous. In fact, consider $q = p_1 \cdot \ldots \cdot p_\kappa$ where $p_1 < \cdots < p_\kappa$ are odd primes. Let $0 = x_1 < x_2 < \cdots < x_{\sigma_q} < q = x_{\sigma_q+1}$ be the squares mod q so that $\sigma_q = \prod_1^\kappa(\frac{p_i+1}{2})$. Let each gap $g_i = x_{i+1} - x_i$ have weight $1/\sigma_q$. The expected gap size is $s_q = \frac{1}{\sigma_q}\sum_1^{\sigma_q} g_i = \frac{q}{\sigma_q} = 2^\kappa \prod_1^\kappa (\frac{p_i}{1+p_i})$. Let us normalize the gaps; $y_i = \frac{g_i}{s_q}$. Kurlberg and Rudnick in [13, Lemma 14] proved the following result. For each $x \in \mathbb{R}$,

$$\lim_{\kappa\to\infty} \frac{\#\{i : y_i \le x\}}{\sigma_q} = 1 - e^{-x}. \tag{52}$$

Choose κ_γ such that if $\kappa > \kappa_\gamma$, then $\frac{\#\{i:\, y_i \le 2\gamma\}}{\sigma_q} < 1 - e^{-3\gamma} < 3\gamma$. For each $\kappa > \kappa_\gamma$ choose $p_{\gamma,\kappa}$ such that if $p_{\gamma,\kappa} < p_1 < \cdots < p_\kappa$ then $\prod_1^\kappa (1 + \frac{1}{p_i}) < 2$ and $\prod_1^\kappa (1 - \frac{1}{p_i}) > 1 - \gamma$. Let $q = p_1 \cdots p_\kappa$. Letting x_i' be the squares modulo q in $[0, q)$ which are not divisible by any of the prime factors of q, we have

(53)

$$\begin{aligned}\overline{\lambda}(\overline{\Lambda}'_\gamma(q)) &\ge \frac{\gamma 2^\kappa}{q} \#\{j : x'_{j+1} - x'_j > \gamma 2^\kappa\} \\ &\ge \frac{\gamma 2^\kappa}{q} \left(\prod_1^\kappa \Big(\frac{p_i - 1}{2}\Big) - \#\{i : y_i \le \frac{\gamma 2^\kappa}{s_q} = \gamma \prod_1^\kappa \Big(1 + \frac{1}{p_i}\Big) < 2\gamma\} \right).\end{aligned}$$

By (52) and our assumptions, we get

$$\begin{aligned}\overline{\lambda}(\overline{\Lambda}'_\gamma(q)) &\ge \gamma \left((1-\gamma) - 3\gamma \prod_1^\kappa \Big(1 + \frac{1}{p_i}\Big) \right) \\ &> \gamma((1-\gamma) - 3\gamma \cdot 2) = \gamma(1 - 7\gamma) = \frac{\gamma}{C_\gamma}.\end{aligned} \tag{54}$$

We have

$$\overline{\lambda}(\overline{\Lambda}'_\gamma(q)) > \gamma(1 - 7\gamma) = 1 - \frac{1 - \gamma - \gamma^2}{\widetilde{C}_\gamma}.$$

So,

$$\frac{1 - \gamma - \gamma^2}{\widetilde{C}_\gamma} > 1 - \overline{\lambda}(\overline{\Lambda}'_\gamma(q)) = \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'_\gamma(q)). \qquad \square$$

In order to apply Lemma 6 we need to choose a positive "leakage constant," γ, which remains fixed during all steps of the leakage producing the $(K+1) - M$ family.

Fixing the leakage constant γ. We choose $0 < \gamma_0 < 10^{-7}$ so that

$$C_{\gamma_0} = \frac{1}{1 - 7\gamma_0} < \Gamma. \tag{55}$$

Moreover, for each $\gamma < \gamma_0$ with $\gamma = 2^{-c_\gamma}$ where $c_\gamma \in \mathbb{N}$, by Lemma 7 we choose κ_γ such that for all $\kappa > \kappa_\gamma$ there exists $p_{\gamma,\kappa}$ for which if $p_{\gamma,\kappa} < p_1 < \cdots < p_\kappa$, $q = p_1 \cdots p_\kappa$, then

$$\overline{\lambda}(\overline{\Lambda}'_\gamma(q)) > \frac{\gamma}{C_{\gamma_0}} = (1 - 7\gamma_0)\gamma > \frac{9\gamma}{10} \text{ and } \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'_\gamma(q)) < 1 - \frac{9\gamma}{10}. \tag{56}$$

We also have,

$$\widetilde{C}_\gamma > 1 - \gamma_0 - \gamma_0^2 > 1 - 10^{-6}.$$

From now on a value of $\gamma < \gamma_0$, with $\gamma = 2^{-c_\gamma}$, $c_\gamma \in \mathbb{N}$ satisfying the above assumptions is fixed.

We note that the only input parameter that the leakage constant depends on is Γ.

We will write $\Lambda(q)$, $\overline{\Lambda}(q)$ and $\overline{\Lambda}'(q)$ instead of $\Lambda_\gamma(q)$, $\overline{\Lambda}_\gamma(q)$ and $\overline{\Lambda}'_\gamma(q)$, respectively.

Next, after giving an outline we start the details of the proof of Lemma 5.

4.2.1. *Setting up the induction argument for Lemma 5.*

Proof. We proceed by mathematical induction. To start our induction we need to show that $1-M$ families exist. During the general step of our induction we show that from the existence of $K-M$ families one can deduce the existence of $(K+1)-M$ families. Since many steps of the $1-M$ family case are shared with the general $K-M$ family case we work out our argument so that it can be used for the later induction steps without any unnecessary duplication. Therefore, working on the first step of our induction one should think of $K=0$ during the first reading of Sections 4.2.2–4.2.8 and obtain this way the $(K+1)-M$, that is, the $1-M$ families. Then in Sections 4.2.9–4.2.15 we discuss the alterations needed for $K>0$. It will be useful to keep in mind that if $K=0$ then $f_{K+1,0} = f_{1,0}$, only $h = 1 \in \{1, \dots, K+1\}$ and there is no $h \in \{1, \dots, K\}$.

Now we discuss briefly our general plan. When $K>0$ we assume that $K-M$ families living on $\mathbb{R}$ exist for all possible input parameter choices. Let $\delta > 0$, Ω, $\Gamma > 1$, $A \in \mathbb{N}$ and $\mathcal{P} \subset \mathbb{N}$ be given. We will define our $(K+1)-M$ family with these input parameters. We can assume that $\mathcal{P}$ is closed under products. During the definition of the $(K+1)-M$ family another, "inner" finite induction is used (with respect to L) which is called the *leakage process*. This technically delicate process is the focus of the next several sections. During this process we will use Lemma 6 to define families which are almost $(K+1)-M$ families on sets of the type $\overline{\Lambda}'(q)$, except for the new functions $f_{K+1,L}$ and $X_{K+1,L}$. Each $f_{K+1,L}$ is the indicator function of a set. As L grows the support of $f_{K+1,L}$ decreases. Lemmas 2 and 3 are used to ensure that "squares hit sufficiently often" the support of $f_{K+1,L}$. (This motivated the term "leakage" since the values of $f_{K+1,L}$ leak onto some larger sets when we consider averages along the squares. See also [8].) This also requires that before defining $f_{K+1,L}$ one uses Lemma 3 to choose τ'_{L-1} and make a τ'_{L-1} rearrangement to yield an intermediate function $f'_{K+1,L-1}$. At the same time we must keep track of our new random variable $X_{K+1,L}$ and other auxiliary functions. It is essential in this induction that we can vary τ and κ.

To help the reader going through the details of the proof here is an outline of the main features of the various sections of the proof. We hope this outline might help prevent the reader from becoming lost in the details of the proof.

When $K = 0$ in Section 4.2.2 we start the leakage process. We define $f_{K+1,0} \equiv 1$ and $X_{K+1,0}$. At this stage $f_{K+1,0}$ is supported on $\mathbb{R}$. During the leakage process the size of the support of the functions $f_{K+1,L}$ is shrinking and we are interested in how much of $f_{K+1,L}$ is "leaking" onto larger sets. When $K > 0$ in Section 4.2.9, in addition, we introduce a $K - M$ family periodic by τ_0, consisting of functions $f_{h,0}$, $X_{h,0}$ for $h = 1, \dots, K$.

In Section 4.2.3 (see also Section 4.2.10 when $K > 0$) we assume that we have accomplished step $L - 1$ of the leakage and we have a family periodic by τ_{L-1}, consisting of functions $f_{h,L-1}$, $X_{h,L-1}$ for $h = 1, \dots, K + 1$. We also introduce the auxiliary sets $S_{L-1,l}$, $l = 0, \dots, L - 1$ used to describe the distribution of $X_{K+1,L-1}$.

In Section 4.2.4 (see also Section 4.2.11 when $K > 0$) we choose a prime number τ'_{L-1} which is much larger than τ_{L-1} and by using Lemma 3 we perform a τ'_{L-1} rearrangement of the family coming from Section 4.2.3. This way we obtain a family periodic by τ'_{L-1}, consisting of functions $f'_{h,L-1}$, $X'_{h,L-1}$, $h = 1, \dots, K+1$. The auxiliary sets used for describing the distribution of $X'_{K+1,L-1}$ are denoted by $S'_{L-1,l}$, $l = 0, \dots, L - 1$.

In Section 4.2.5 we choose a κ_L and a square free number $q_L = p_{1,L} \cdots q_{\kappa_L,L}$ such that 2^{κ_L} is much larger than τ'_{L-1}. The average value of the difference between elements of $\Lambda_0(q_L)$ is close to 2^{κ_L}. We introduce some auxiliary sets, among them Φ_L and Ψ_L, so that $\Phi_L \subset \mathbb{R} \setminus \overline{\Lambda}'(q_L) \subset \Psi_L$ and these two auxiliary sets consist of intervals of the form $[j\tau'_{L-1}, (j + 1)\tau'_{L-1})$, $j \in \mathbb{Z}$. If 2^{κ_L} is much larger than τ'_{L-1}, then $\overline{\lambda}(\Phi_L)$ and $\overline{\lambda}(\Psi_L)$ both approximately equal $\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L))$. To define our $(K + 1) - M$ family on Ψ_L (which is approximately $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$) we will use mainly the functions coming from Section 4.2.4. We define $X_{h,L}(x) = X'_{h,L-1}(x)$ if $h \le K + 1$ and $x \in \Phi_L$. This section is identical for the cases $K = 0$ and $K > 0$.

For $K > 0$ in Section 4.2.13 by using Lemma 6 we put a $K - M$ family onto $\overline{\Lambda}'(q_L)$. This will yield functions $\overline{f}_{h,L}$, $\overline{X}_{h,L}$ periodic by $\overline{\tau}_L q_L$. For $h = 1, \dots, K$ we define $X_{h,L}$ on $\overline{\Lambda}'(q_L)$ by using $\overline{X}_{h,L}$. For $h = 1, \dots, K$ our functions will be sums of $f'_{h,L-1}$ restricted to Φ_L and of the functions $\overline{f}_{h,L}$ "living" on $\overline{\Lambda}'(q_L)$. This combined family will be periodic by $\tau_L = q_L \overline{\tau}_L \tau'_{L-1}$. The $K = 0$ version discussed in Section 4.2.6 is much simpler because we do not have to deal with this putting a lower level family on the $\overline{\Lambda}'(q_L)$ step.

The "leakage" is done when we define $f_{K+1,L}$ so that it equals the restriction of $f'_{K+1,L-1}$ onto the set Ψ_L. This means that the support F_L of $f_{K+1,L}$ will have a very small intersection with $\overline{\Lambda}'(q_L)$. "Most" of F_L will be a subset of $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$ and will approximately equal the auxiliary set $S_{L,0}$. The nested sequence $S_{L,l}$, $l = 0, \ldots, L$ will describe the distribution $X_{K+1,L}$, the larger l, the smaller the values $X_{K+1,L}$ can take on $S_{L,l} \setminus S_{L,l-1}$.

In Section 4.2.7 we make the calculations needed to show that we have enough "leakage" from the support of $f_{K+1,L}$ so that we have the domination inequality (37) with $f_{K+1,L}$ and $X_{K+1,L}$. This section is again the same for the cases $K = 0$ and $K > 0$.

Finally, in Section 4.2.8 (see also Section 4.2.15 when $K > 0$) we terminate the leakage process when we have reached a suitably large $L = L'' \leq L'$. The functions $f_{h,L''}$ for $h = 1, \ldots, K+1$ will yield the functions f_h we need for the $(K+1) - M$ family. For $h = 1, \ldots, K$ the functions X_h of the $(K+1) - M$ family will equal the functions $X_{h,L''}$. To define X_{K+1} we use the sets $S_{L'',l}$, $l = 0, \ldots, L''$ related to the distribution of $X_{K+1,L''}$. We will choose X_{K+1} so that it is M−0.99 distributed and less or equal than $X_{K+1,L''}$.

Before turning to the details of the induction to help the reader going through the details of the proof for easy reference we collect some definitions and properties (some of them will be discussed later during the proof) at the same place.

Quick reference summary:

$$\Lambda(q) = \Lambda_\gamma(q) = -\Lambda_0(q) + \{j \in \mathbb{Z} : 0 \leq j < \gamma 2^\kappa\},$$
$$\overline{\Lambda}(q) = \overline{\Lambda}_\gamma(q) = \Lambda_\gamma(q) + [0,1) = -\Lambda_0(q) + \{x : 0 \leq x < \gamma 2^\kappa\},$$
$$\Lambda'_0(q) = \{n \in \Lambda_0(q) : p_j \not| n, \text{ for all } j = 1, \ldots, \kappa\},$$
$$\Lambda'(q) = \Lambda'_\gamma(q) = -\Lambda'_0(q) + \{j \in \mathbb{Z} : 0 \leq j < \gamma 2^\kappa\},$$
$$\overline{\Lambda}'(q) = \overline{\Lambda}'_\gamma(q) = \Lambda'_\gamma(q) + [0,1) = -\Lambda'_0(q) + \{x : 0 \leq x < \gamma 2^\kappa\}.$$

At Step $L = 0$ of the leakage process we have: $f_{K+1,0} \equiv 1$, $F_0 = \mathbb{R}$, $S_{0,0} = \mathbb{R}$, $r_0 = 1$, $X_{K+1,0} \stackrel{\text{def}}{=} (1-\rho')\widetilde{C}_\gamma = (1-\rho')\widetilde{C}_\gamma \overline{\lambda}(F_0) < 1$.

After Step $L-1$ of the leakage process we have: The set F_{L-1}, an exceptional set E^{L-1}, a period τ_{L-1} such that F^{L-1}, E^{L-1}, $X_{h,L-1}$, $f_{h,L-1}$, $(h = 1, \ldots, K+1)$ are periodic by τ_{L-1}, $f_{h,L-1} : \mathbb{R} \to [0,\infty)$, the "random" variables $X_{h,L-1} : \mathbb{R} \to \mathbb{R}$ are pairwise independent for $h = 1, \ldots, K+1$, $X_{h,L-1}$ are M−0.99-distributed for $h = 1, \ldots, K$, but not for $h = K+1$. For the distribution of $X_{K+1,L-1}$ the auxiliary sets $S_{L-1,l}$ are used. For all $x \notin E^{L-1}$ there exist $\omega_{L-1}(x) > \alpha_{L-1}(x) > A$, $\tau_{L-1}(x) < \tau_{L-1}$.

Then we do a τ'_{L-1} periodic rearrangement. We choose and fix a sufficiently large prime τ'_{L-1}. The set $F_{L-1}^{\tau'_{L-1}}$ is the τ'_{L-1} periodic rearrangement of F_{L-1}. We modify our sets and functions so that they are all periodic with respect to τ'_{L-1}.

The new functions are: $f'_{h,L-1}\ \alpha'_{L-1}(x)\ \omega'_{L-1}(x)\ \tau'_{L-1}(x)\ X'_{h,L-1}(x)$. We define ${E'}^{L-1}$ so that it satisfies (72). We set $S'_{L-1,L-1} = \mathbb{R}$ and define the sets $S'_{L-1,l}$. These sets are used in (75) for the distribution of $X'_{K+1,L-1}$.

Then we choose a sufficiently large q_L, and several important auxiliary sets: $\bar{\Xi}(q_L) = \cup_{j\in\mathbb{Z}}[jq_L, jq_L + \gamma 2^{\kappa_L})$,
$\widetilde{\Phi}_L = \{x : \mathrm{dist}(x, \overline{\Lambda}'(q_L) \cup \bar{\Xi}(q_L)) > 2\tau'_{L-1}\}$,
$\Phi_L = \cup\{[j\tau'_{L-1}, (j+1)\tau'_{L-1}) : \widetilde{\Phi}_L \cap [j\tau'_{L-1}, (j+1)\tau'_{L-1}) \neq \varnothing\}$, which satisfy: $\widetilde{\Phi}_L \subset \Phi_L \subset \widehat{\Phi}_L \subset \mathbb{R} \setminus \overline{\Lambda}'(q_L) \subset \widehat{\Psi}_L \subset \Psi_L \subset \widetilde{\Psi}_L$ The sets Φ_L and Ψ_L are periodic by $\tau'_{L-1}q_L$ and the sets $\widetilde{\Phi}_L$, $\widehat{\Phi}_L$, $\widetilde{\Psi}_L$, and $\widehat{\Psi}_L$ are periodic by q_L. They satisfy (90). We put $E'_L = \Psi_L \cap {E'}^{L-1}$, $E''_L = \mathbb{R} \setminus (\overline{\Lambda}'(q_L) \cup \widetilde{\Phi}_L)$ and $\widetilde{E}''_L = \mathbb{R} \setminus (\overline{\Lambda}'(q_L) \cup \Phi_L) \subset E''_L$. The set E''_L is periodic by q_L, while $\widetilde{E}''_L$ is periodic by $\tau'_{L-1}q_L$. The exceptional set $\overline{E}'''_L$ is defined at (112) and E'''_L in (114).

From this place on our definition of our new objects, like the functions $f_{h,L}$ and $X_{h,L}$ splits and follows two different paths. One will be the definition of these objects on $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$ and the other the definition of these objects on $\overline{\Lambda}'(q_L)$.

For the first path we are unable to use exactly the set $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$. We need to use the auxiliary sets Φ_L and Ψ_L which are good approximations of this set. We have for example $f_{K+1,L} = f'_{K+1,L-1}\chi_{\Psi_L}$.

For the second path by our induction assumption we put a $K-M$-family on $\overline{\Lambda}'(q_L)$. The sets and functions obtained at this step are periodic by $\overline{\tau}_L q_L$. They are $\overline{f}_{h,L}$, $\overline{\alpha}_L$, $\overline{\omega}_L$, $\overline{\tau}_L$, $\overline{X}_{h,L}$ and there is an exceptional set $E_{\delta,L}$.

We combine these two paths when we define $f_{h,L} = f'_{h,L-1} \cdot \chi_{\Phi_L} + \overline{f}_{h,L}$ for $h = 1, \ldots, K$.

Quick reference summary ends here.

Next we turn to the details of our argument. We start by choosing some constants.

Choose a positive integer L' such that

$$\left(1 - \frac{\gamma}{2}\right)^{L'} < \frac{1}{2^M}. \tag{57}$$

By recursion we construct pairs of functions $f_{K+1,0}, X_{K+1,0}, \ldots, f_{K+1,L}, X_{K+1,L}$ and some associated objects. The inner finite induction, the "leakage" will halt at some step $L'' \le L'$. We show that the functions $f_{K+1,L''}, X_{K+1,L''}$ and their associated objects form a $(K+1)-M$ family except for the distribution of $X_{K+1,L''}$. However we will know enough about its distribution to easily obtain a $(K+1)-M$ family.

By (55) we have $C_\gamma < C_{\gamma_0} < \Gamma$.

We recall that the only input parameter that the leakage constant depends on is Γ. This dependence, and the possibility of using different values for Γ will play an important role during the definition of $(K+1)-M$ families with $K>0$.

Fix a constant $\Gamma_0 > 1$ such that

$$C_\gamma \Gamma_0 < \Gamma. \tag{58}$$

Put

$$\delta_L = \frac{\delta}{4(L'+1)} \text{ for } L = 0, \dots, L'.$$

Next we choose sufficiently small positive constants ρ, ρ' and $\widetilde{\rho}$.

We suppose that

$$(1-\rho)(1-2\gamma) > 1-3\gamma. \tag{59}$$

Recall that $1 > \widetilde{C}_\gamma > 1-10^{-6}$ and we choose $\rho' > 0$ such that

$$0.999 < \widetilde{C}_\gamma (1-\rho') < 1 < 1.001. \tag{60}$$

Since $0 < \gamma < \gamma_0 < 10^{-7}$ and $1 > \widetilde{C}_\gamma > 1-10^{-6}$ we can suppose that ρ and ρ' are so small that

$$(1-\rho)^2(1-2\gamma)^2(1-\rho')\widetilde{C}_\gamma - \frac{(1-\rho')\widetilde{C}_\gamma}{0.999\cdot(1-\rho)^2}\cdot\frac{1}{2} > 0.99\cdot\frac{1}{2}. \tag{61}$$

Moreover, choose $\widetilde{\rho} > 0$ such that

$$\left(1-\frac{\rho'}{2}\right)(1-2\widetilde{\rho}) > 1-\rho'. \tag{62}$$

Finally, we set $\mathcal{P}_0 = \mathcal{P} \cup \mathcal{P}'_0 \cup \dots \cup \mathcal{P}'_{L'}$ where $\mathcal{P}$ and each $\mathcal{P}'_j$ contains infinitely many primes and all their possible products, but numbers in different sets are relatively prime; moreover $\mathcal{P}_0$ has sufficiently large complement.

4.2.2. *Step $L=0$ of the leakage process.* We put $f_{K+1,0} \equiv 1$. Set $F_0 = \mathbb{R}$, $S_{0,0} = \mathbb{R}$, $r_0 = 1$. So, $\overline{\lambda}(F_0) = 1$ and $X_{K+1,0} \overset{\text{def}}{=} (1-\rho')\widetilde{C}_\gamma = (1-\rho')\widetilde{C}_\gamma\overline{\lambda}(F_0) < 1$, see (60).

For the case $K=0$ we use the following argument. For $K>0$ see a different argument in 4.2.9.

We choose a sufficiently large τ_0, and functions $\alpha_0(x)$, $\omega_0(x)$, $\tau_0(x)$ taking integer values for all $x \in \mathbb{R}$ (in fact, these functions can be constant on $\mathbb{R}$), such that the following assumptions hold: $\omega_0(x) > \alpha_0(x) > A$, $\tau_0(x) < \tau_0$, $\omega_0^2(x) < \tau_0$, $\frac{\omega_0(x)}{\alpha_0(x)} > \Omega\tau_0(x) = \Omega_0\tau_0(x)$, and for all $p \in \mathcal{P}_0$, $(\tau_0(x), p) = 1$, $(\tau_0, p) = 1$. For example, we could take $\alpha_0(x) = A+1$, $\tau_0(x)$ to be the smallest odd prime which is relatively prime to all elements of $\mathcal{P}_0$, $\omega_0(x) = \tau_0(x)\Omega(A+2)$ and τ_0 be the smallest prime relatively prime to the elements of $\mathcal{P}_0$ and greater than $(\omega_0(x))^2$.

By our choices; $f_{K+1,0} = f_{1,0} \equiv 1$. We put $E_{\delta_0} = \varnothing$ and $E^0 = \varnothing$. For any $m \in \mathbb{N}$ we have the all important "domination" property: for all $x \in \mathbb{R} \setminus E^0$,

$$\frac{1}{m} \sum_{k=n}^{n+m-1} f_{1,0}(x + k^2) > X_{1,0}(x).$$

It is also clear that for all $x \in \mathbb{R}$, $f_{1,0}(x + j + \tau_0(x)) = f_{1,0}(x + j)$ for any $j \in \mathbb{R}$.

4.2.3. *The setting after step $L - 1$ of the leakage.* Assume we have accomplished step $L - 1$ of the leakage process. We have constructed some objects satisfying the following conditions. There is an exceptional set E^{L-1} with

(63) $$\overline{\lambda}(E^{L-1}) < \frac{L}{(L' + 1)}\delta;$$

$\mathcal{P}_{L-1} = \mathcal{P} \cup \mathcal{P}'_L \cup \cdots \cup \mathcal{P}'_{L'}$; there exists a period τ_{L-1} such that E^{L-1}, $X_{h,L-1}$, $f_{h,L-1}$, $(h = 1, \dots, K + 1)$ are periodic by τ_{L-1}, $f_{h,L-1} : \mathbb{R} \to [0, \infty)$, (for $K > 0$) the "random" variables $X_{h,L-1} : \mathbb{R} \to \mathbb{R}$ are pairwise independent for $h = 1, \dots, K + 1$, $X_{h,L-1}$ are M–0.99-distributed for $h = 1, \dots, K$ (in (67)–(70) we list the assumptions about the distribution of $X_{K+1,L-1}$, recall that for $K = 0$ there is no h satisfying $h = 1, \dots, K$). For all $x \notin E^{L-1}$ there exist $\omega_{L-1}(x) > \alpha_{L-1}(x) > A$, $\tau_{L-1}(x) < \tau_{L-1}$ such that $\omega^2_{L-1}(x) < \tau_{L-1}$, $\frac{\omega_{L-1}(x)}{\alpha_{L-1}(x)} > \Omega\tau_{L-1}(x)$; moreover if $\alpha_{L-1}(x) \le n < n + m \le \omega_{L-1}(x)$ and $\tau_{L-1}(x)|m$, then for all $h = 1, \dots, K + 1$,

(64) $$\frac{1}{m} \sum_{k=n}^{n+m-1} f_{h,L-1}(x + k^2) > X_{h,L-1}(x);$$

for all $p \in \mathcal{P}_{L-1}$, $(\tau_{L-1}(x), p) = 1$, $(\tau_{L-1}, p) = 1$; moreover for all $x \notin E^{L-1}$, $f_{h,L-1}(x+j+\tau_{L-1}(x)) = f_{h,L-1}(x+j)$ whenever $\alpha^2_{L-1}(x) \le j < j+\tau_{L-1}(x) \le \omega^2_{L-1}(x)$ for all $h \in \{1, \dots, K + 1\}$.

We suppose that the values of $f_{K+1,L-1}$ are 0 or 1, that is, it is an indicator function.

If $L - 1 = 0$, then $X_{K+1,L-1}$ is constant.

If $L - 1 > 0$, that is, $L \ge 2$ then we give the extra assumptions about the distribution of $X_{K+1,L-1}$ as follows.

Recall $F_0 = \mathbb{R}$ and also recall that for a Lebesgue measurable set F, periodic by p we have $\overline{\lambda}(F) = \frac{1}{p}\lambda(F \cap [0, p)) = \lim_{N\to\infty} \frac{\lambda(F\cap[-N,N])}{2N}$. We suppose that the sets F_l periodic by τ_l and the numbers r_l have been defined for $l = 0, \dots, L-2$ during the previous steps of our induction,

(65) $$\frac{\overline{\lambda}(F_l)}{\overline{\lambda}(F_{l-1})} = r_l \text{ and } 1 - 2\gamma < r_l < 1 - \frac{\gamma}{2}$$

hold for $l = 1, \dots, L-1$. Clearly, $\overline{\lambda}(F_l) = r_0 \cdots r_l$. We also have τ_l periodic functions $f_{K+1,l} = \chi_{F_l}$ for each $0 \le l \le L-1$.

Set $F_{L-1} = \{x : f_{K+1,L-1}(x) = 1\}$ and $r_{L-1} = \frac{\overline{\lambda}(F_{L-1})}{\overline{\lambda}(F_{L-2})} < 1$. We also assume

$$1 - 2\gamma < r_{L-1} < 1 - \frac{\gamma}{2}, \tag{66}$$

$\overline{\lambda}(F_{L-1}) = r_1 \cdots r_{L-1} = r_0 \cdots r_{L-1}$. In (103) we explicitly show that this holds for r_1. The sets $S_{L-1,0} \subset \ldots \subset S_{L-1,L-1} = \mathbb{R}$ are defined so that

$$\frac{1}{1-\rho}\overline{\lambda}(F_{L-1}) > \overline{\lambda}(S_{L-1,0}) > (1-\rho)\overline{\lambda}(F_{L-1}), \tag{67}$$

if $x \in S_{L-1,0}$ then $X_{K+1,L-1}(x) = (1-\rho')\widetilde{C}_\gamma = (1-\rho')\widetilde{C}_\gamma\overline{\lambda}(F_0)$. For $l = 0, \dots, L-1$ we have

$$\frac{1}{(1-\rho)r_0 \cdots r_l}\overline{\lambda}(S_{L-1,0}) > \overline{\lambda}(S_{L-1,l}) > \frac{1-\rho}{r_0 \cdots r_l}\overline{\lambda}(S_{L-1,0}), \tag{68}$$

which is equivalent to

$$\frac{1}{(1-\rho)}\overline{\lambda}(S_{L-1,0}) > \overline{\lambda}(F_l) \cdot \overline{\lambda}(S_{L-1,l}) > (1-\rho)\overline{\lambda}(S_{L-1,0}). \tag{69}$$

If $x \in S_{L-1,l} \setminus S_{L-1,l-1}$ for $l \in \{1, \dots, L-1\}$, then

$$X_{K+1,L-1}(x) = (1-\rho')r_0 \cdots r_l\widetilde{C}_\gamma = (1-\rho')\overline{\lambda}(F_l)\widetilde{C}_\gamma. \tag{70}$$

The sets $S_{L-1,l}$ are increasing almost by a factor $1/r_l$ in size, whereas the value of $X_{K+1,L-1}$ on the difference is decreasing by a factor r_l. We also assume that F_{L-1} has the property that if $x \in F_{L-1}$ then $[\lfloor x \rfloor, \lfloor x \rfloor + 1) \subset F_{L-1}$.

We note that by (65)

$$\overline{\int} f_{K+1,l} \le \left(1 - \frac{\gamma}{2}\right)^l \text{ for } l = 0, \dots, L-1.$$

4.2.4. *Rearrangement with respect to τ'_{L-1}, choice of τ'_{L-1}.* In order to construct the next set of objects in the recursion, we first create, by rearrangement, some associated objects to the $(L-1)$-st step which are denoted by attaching primes.

Since the set F_{L-1} is periodic by τ_{L-1} and is the union of some integral intervals we can apply Lemma 3. We choose $M_{\rho'/2}$ such that for all prime numbers $\tau'_{L-1} > M_{\rho'/2}$ if we consider $F_{L-1}^{\tau'_{L-1}}$, the τ'_{L-1} periodic rearrangement of F_{L-1}, then for any $x \in \mathbb{R}$ if $\tau'_{L-1} | m$, then

$$\frac{1}{m}\sum_{k=n}^{n+m-1} \chi_{F_{L-1}^{\tau'_{L-1}}}(x+k^2) \ge \left(1 - \frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1}). \tag{71}$$

We will choose and fix a sufficiently large prime $\tau'_{L-1} \in \mathcal{P}'_{L-1}$. We define the numbers $\mathcal{T}_i$, $i = 1, \dots, 5$ below. We choose τ'_{L-1} so that it is larger than the maximum of $\mathcal{T}_1, \dots, \mathcal{T}_5$ and $M_{\rho'/2}$. Hence (71), (73), (76), (77), (78), (80), (81), and (82) hold.

Now, we modify our sets and functions so that they are all periodic with respect to τ'_{L-1}. Since we are going to define functions which are periodic by τ'_{L-1}, it is sufficient to define them on $[0, \tau'_{L-1})$.

If $x \in [0, \lfloor \tau'_{L-1}/\tau_{L-1} \rfloor \cdot \tau_{L-1})$ and the right-hand side of the equation is defined at x, set

$$\begin{aligned} f'_{h,L-1}(x) &= f_{h,L-1}(x), \ h = 1, \dots, K+1, \\ \alpha'_{L-1}(x) &= \alpha_{L-1}(x), \\ \omega'_{L-1}(x) &= \omega_{L-1}(x), \\ \tau'_{L-1}(x) &= \tau_{L-1}(x), \\ X'_{h,L-1}(x) &= X_{h,L-1}(x), \ h = 1, \dots, K+1. \end{aligned}$$

On $[\lfloor \tau'_{L-1}/\tau_{L-1} \rfloor \tau_{L-1}, \tau'_{L-1})$ we define all the above functions equal to zero with the exception of the functions $X'_{h,L-1}$, $h = 1, \dots, K+1$.

When $K > 0$ for these functions some minor adjustments will be made on this interval in order to ensure that they are pairwise independent for $h = 1, \dots, K+1$ and are M−0.99-distributed for $h = 1, \dots, K$.

We can also assume that $X'_{K+1,L-1}$ has constant value $(1-\rho')\overline{\lambda}(F_{L-1})\widetilde{C}_\gamma$ on $[\lfloor \tau'_{L-1}/\tau_{L-1} \rfloor \tau_{L-1}, \tau'_{L-1})$. When $L-1 = 0$ then this implies that $X'_{K+1,L-1}$ takes this constant value on $\mathbb{R}$.

We define E'^{L-1} so that it is periodic by τ'_{L-1} and

(72)

$$\begin{aligned} &E'^{L-1} \cap [0, \tau'_{L-1}) \\ &\quad = \left(E^{L-1} \cap \left[0, \left(\left\lfloor \frac{\tau'_{L-1}}{\tau_{L-1}} \right\rfloor - 1 \right) \tau_{L-1} \right) \right) \cup \left[\left(\left\lfloor \frac{\tau'_{L-1}}{\tau_{L-1}} \right\rfloor - 1 \right) \tau_{L-1}, \tau'_{L-1} \right). \end{aligned}$$

By choosing τ'_{L-1} sufficiently large we can make $0 \le \overline{\lambda}(E'^{L-1}) - \overline{\lambda}(E^{L-1})$ as small as we wish, hence, using (63) there is $\mathcal{T}_1$ such that if $\tau'_{L-1} > \mathcal{T}_1$, then

$$\overline{\lambda}(E'^{L-1}) < \frac{L}{(L'+1)}\delta. \tag{73}$$

When $L - 1 = 0$ then

$$X'_{K+1,0}(x) = (1-\rho')\overline{\lambda}(F_0)\widetilde{C}_\gamma \text{ for all } x \in \mathbb{R}. \tag{74}$$

If $L - 1 > 0$, that is, $L \ge 2$ we need to deal with the auxiliary sets related to the distribution of $X'_{K+1,L-1}$. We put $S'_{L-1,L-1} = \mathbb{R}$. Observe that (72) holds with ${E'}^{L-1}$, E^{L-1} being replaced by $S'_{L-1,L-1}$, and $S_{L-1,L-1}=\mathbb{R}$, respectively. For $l=0,\dots,L-2$ we define the sets $S'_{L-1,l}$ so that they are periodic by τ'_{L-1} and we have

$$S'_{L-1,l}\cap[0,\tau'_{L-1})=S_{L-1,l}\cap[0,(\lfloor\tau'_{L-1}/\tau_{L-1}\rfloor-1)\tau_{L-1}).$$

The above definitions and (70) imply

(75)

$$X'_{K+1,L-1}(x)=(1-\rho')\widetilde{C}_\gamma\overline{\lambda}(F_0)\text{ for }x\in S'_{L-1,0},$$

and

$$X'_{K+1,L-1}(x)=(1-\rho')\widetilde{C}_\gamma\overline{\lambda}(F_l)\text{ for }x\in S'_{L-1,l}\setminus S'_{L-1,l-1},\ l=1,\dots,L-1.$$

By the strict inequalities in (67), (68) and (69) we can choose $\mathcal{T}_2$ such that if $\tau'_{L-1}>\mathcal{T}_2$ then

$$\frac{1}{1-\rho}\overline{\lambda}(F_{L-1})>\overline{\lambda}(S'_{L-1,0})>(1-\rho)\overline{\lambda}(F_{L-1})\tag{76}$$

and for $l=0,\dots,L-1$

$$\frac{1}{(1-\rho)r_0\cdots r_l}\overline{\lambda}(S'_{L-1,0})>\overline{\lambda}(S'_{L-1,l})>(1-\rho)\frac{1}{r_0\cdots r_l}\overline{\lambda}(S'_{L-1,0}),\tag{77}$$

or, equivalently,

$$\frac{1}{1-\rho}\overline{\lambda}(S'_{L-1,0})>\overline{\lambda}(F_l)\cdot\overline{\lambda}(S'_{L-1,l})>(1-\rho)\overline{\lambda}(S'_{L-1,0}).\tag{78}$$

Set $F'_{L-1}=\{x:f'_{K+1,L-1}(x)=1\}$, that is, $F'_{L-1}\cap[0,\tau'_{L-1})=F_{L-1}\cap[0,\lfloor\tau'_{L-1}/\tau_{L-1}\rfloor\tau_{L-1})=F_{L-1}^{\tau'_{L-1}}\cap[0,\lfloor\tau'_{L-1}/\tau_{L-1}\rfloor\tau_{L-1})$ and $f'_{K+1,L-1}(x)=\chi_{F_{L-1}^{\tau'_{L-1}}}(x)$ for all $x\in\mathbb{R}$. Clearly, $\overline{\lambda}(F'_{L-1})\le\overline{\lambda}(F_{L-1})$.

For the case $L-1=0$ we note that $F_0\cap[0,\tau'_{L-1})=[0,\lfloor\tau'_{L-1}/\tau_{L-1}\rfloor\tau_{L-1})$.

By (71) for any $x\in\mathbb{R}$ from $\tau'_{L-1}|m$, it follows that letting $f'_{K+1,L-1}=\chi_{F_{L-1}^{\tau'_{L-1}}}$ we have

$$\frac{1}{m}\sum_{k=n}^{n+m-1}f'_{K+1,L-1}(x+k^2)>\left(1-\frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1}).\tag{79}$$

This formula is the main motivation for introducing the τ'_{L-1} periodic rearrangements.

Observe that if $\tau'_{L-1}\to\infty$ then $\overline{\lambda}(F'_{L-1})/\overline{\lambda}(F_{L-1})\to1$.

Hence we can choose $\mathcal{T}_3$ such that if $\tau'_{L-1} > \mathcal{T}_3$, then

$$1-\rho < \frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})} \le 1. \tag{80}$$

We remark that for $L-1=0$ inequality (80) simply means $1-\rho < \overline{\lambda}(F'_0)$.

Moreover, we can choose $\mathcal{T}_4$ such that if $\tau'_{L-1} > \mathcal{T}_4$, then

$$1-\frac{\gamma}{10} < \frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})} \le 1 < 1+\frac{\gamma}{10}. \tag{81}$$

Finally, by (67) and (76) if $L \ge 2$ we can choose $\mathcal{T}_5$ such that if $\tau'_{L-1} > \mathcal{T}_5$ then

$$\frac{1}{1-\rho}\overline{\lambda}(F'_{L-1}) > \overline{\lambda}(S'_{L-1,0}) > (1-\rho)\overline{\lambda}(F'_{L-1}) \tag{82}$$

holds as well.

If $x \in [0, \tau'_{L-1}) \setminus E'^{L-1}$, then put $\alpha'_{L-1}(x) = \alpha_{L-1}(x)$, $\omega'_{L-1}(x) = \omega_{L-1}(x)$, $\tau'_{L-1}(x) = \tau_{L-1}(x) < \tau_{L-1} \ll \tau'_{L-1}$. This defines $\alpha'_{L-1}(x)$, $\omega'_{L-1}(x)$, and $\tau'_{L-1}(x)$ for all $x \in \mathbb{R} \setminus E'^{L-1}$ as well since these functions are periodic by τ'_{L-1}. It is also clear that $(\tau'_{L-1}(x), p) = 1$ for all $p \in \mathcal{P}_{L-1}$. We have $(\omega'_{L-1}(x))^2 < \tau_{L-1}$ and

$$\frac{\omega'_{L-1}(x)}{\alpha'_{L-1}(x)} > \Omega\tau'_{L-1}(x). \tag{83}$$

Suppose $\alpha'_{L-1}(x) \le n < n+m \le \omega'_{L-1}(x)$ and $\tau'_{L-1}(x) = \tau_{L-1}(x)|m$. Since $x \notin E'^{L-1}$, formula (72) implies that $x+k^2 \in [0, \lfloor \tau'_{L-1}/\tau_{L-1}\rfloor \tau_{L-1})$ for $k \in \{n, \dots, n+m-1\}$ we infer by (64) for $h = 1, \dots, K+1$

$$\begin{aligned}\frac{1}{m}\sum_{k=n}^{n+m-1} f'_{h,L-1}(x+k^2) &= \frac{1}{m}\sum_{k=n}^{n+m-1} f_{h,L-1}(x+k^2) \\ &> X_{h,L-1}(x) = X'_{h,L-1}(x).\end{aligned} \tag{84}$$

For all $x \in [0, \tau'_{L-1}) \setminus E'^{L-1}$, $h \in \{1, \dots, K+1\}$, if $\alpha'^2_{L-1}(x) \le j < j+\tau'_{L-1}(x) \le \omega'^2_{L-1}(x)$, $f_{h,L-1}(x+j+\tau_{L-1}(x)) = f'_{h,L-1}(x+j+\tau'_{L-1}(x)) = f'_{h,L-1}(x+j) = f_{h,L-1}(x+j)$. By periodicity with respect to τ'_{L-1}, the above estimates hold for any $x \notin E'^{L-1}$.

4.2.5. *Choice of* κ_L, q_L, Φ_L, Ψ_L, *and* $X_{h,L}$ *on* $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$. Our goal in this section is to describe some sets, in particular Φ_L and Ψ_L, so that we can take $f_{K+1,L} = f'_{K+1,L-1}\chi_{\Psi_L}$ in Section 4.2.6. The functions $f'_{K+1,L-1}$ and χ_{Ψ_L} are "independent" which allows us to reduce the integral of $f_{K+1,L}$. In this section we construct three components of the next exceptional set E^L. The fourth component will be defined in Section 4.2.13. This last component is the exceptional set coming from the $K-M$ family which we put on $\overline{\Lambda}'(q_L)$. We also construct the function $X_{K+1,L}$. To construct the sets mentioned above we choose a number $q_L \in \mathcal{P}'_L$, $q_L = p_{1,L} \cdots p_{\kappa_L,L}$, $p_{1,L} < \cdots < p_{\kappa_L,L}$, where κ_L and $p_{1,L}$ are both sufficiently large.

In fact, we will suppose that κ_L is larger than the maximum of the numbers $\mathcal{K}_i$, $i = 1, \dots, 7$ and κ_γ, we also suppose that $p_{1,L}$ is larger than the maximum of $\pi_i(\kappa_L)$, $i = 0, \dots, 7$, $p''_{1,L}$, and $p_{\gamma,\kappa}$, where $\mathcal{K}_i$, π_i and $p''_{1,L}$ are defined below, the numbers κ_γ and $p_{\gamma,\kappa}$ were defined in Lemma 7. With these assumptions we will be able to use (85), (92), (94), (98), (100), (102), (107), and (113) simultaneously.

Recall that we assumed that $\widetilde{\rho} > 0$ satisfies (62). An application of Lemma 2 with κ_L, $\epsilon = \delta/4L'$ and $\widetilde{\rho}$ instead of ρ yields $p''_{1,L}$ sufficiently large so that $q_L = p_{1,L} \cdots p_{\kappa_L,L}$, with $p''_{1,L} < p_{1,L}$ satisfies (14) and hence we will be able to use (113).

By (36) for given κ_L we can choose $\pi_0(\kappa_L)$ such that for $p_{1,L} > \pi_0(\kappa_L)$ we have

$$\#((\Lambda_0(q_L) \setminus \Lambda'_0(q_L)) \cap [0, q_L)) < \widetilde{\rho}(1-\gamma)\#(\Lambda_0(q_L) \cap [0, q_L)). \tag{85}$$

Recall from Remark 1 that the average gap length between points of $\Lambda_0(q_L)$ is approximately 2^{κ_L} and we can assume that it is much larger than τ'_{L-1}. The normalized difference between elements of $\Lambda_0(q_L)$ approximates Poisson distribution by the results in [13], see also Lemma 7. We also recall from Lemma 6 that $\overline{\Xi}(q_L) = \cup_{j \in \mathbb{Z}}[jq_L, jq_L + \gamma 2^{\kappa_L})$. We put

$$\widetilde{\Phi}_L = \{x : \operatorname{dist}(x, \overline{\Lambda}'(q_L) \cup \overline{\Xi}(q_L)) > 2\tau'_{L-1}\}, \tag{86}$$

$$\begin{aligned} \Phi_L &= \cup\{[j\tau'_{L-1}, (j+1)\tau'_{L-1}) : \widetilde{\Phi}_L \cap [j\tau'_{L-1}, (j+1)\tau'_{L-1}) \neq \varnothing\}, \\ \widehat{\Phi}_L &= \{x : \operatorname{dist}(x, \overline{\Lambda}'(q_L)) > \tau'_{L-1}\}, \\ \widehat{\Psi}_L &= \{x : \operatorname{dist}(x, \mathbb{R} \setminus \overline{\Lambda}'(q_L)) \leq \tau'_{L-1}\}, \\ \Psi_L &= \cup\{[j\tau'_{L-1}, (j+1)\tau'_{L-1}) : \widehat{\Psi}_L \cap [j\tau'_{L-1}, (j+1)\tau'_{L-1}) \neq \varnothing\}, \end{aligned} \tag{87}$$

and finally

$$\widetilde{\Psi}_L = \{x : \operatorname{dist}(x, \mathbb{R} \setminus \overline{\Lambda}'(q_L)) \leq 2\tau'_{L-1}\}.$$

It is clear that

$$\widetilde{\Phi}_L \subset \Phi_L \subset \widehat{\Phi}_L \subset \mathbb{R} \setminus \overline{\Lambda}'(q_L) \subset \widehat{\Psi}_L \subset \Psi_L \subset \widetilde{\Psi}_L. \tag{88}$$

It is also important that by (86) and (87) we have

$$\Phi_L \cap \overline{\Xi}(q_L) = \varnothing. \tag{89}$$

The sets Φ_L and Ψ_L are periodic by $\tau'_{L-1}q_L$ and the sets $\widetilde{\Phi}_L$, $\widehat{\Phi}_L$, $\widetilde{\Psi}_L$, and $\widehat{\Psi}_L$ are periodic by q_L. If κ_L is sufficiently large, then 2^{κ_L} and hence most of the gaps between points of $\Lambda_0(q_L)$ are much larger than τ'_{L-1}. In the sequel by $\approx$ we mean that if $p_{1,L}$ and 2^{κ_L} (compared to τ'_{L-1}) are sufficiently large, then the ratio of the two sides of $\approx$ is sufficiently close to 1, later we will specify further this assumption. Since $\overline{\Lambda}'(q_L)$ consists of intervals of length $\gamma 2^{\kappa_L}$ which is much larger than τ'_{L-1}, we have

$$\overline{\lambda}(\widetilde{\Psi}_L) \approx \overline{\lambda}(\widetilde{\Phi}_L) \approx \overline{\lambda}(\Psi_L) \approx \overline{\lambda}(\Phi_L) \approx \overline{\lambda}(\widehat{\Psi}_L) \approx \overline{\lambda}(\widehat{\Phi}_L), \tag{90}$$

$$\overline{\lambda}(\Phi_L) \leq \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L)) \leq \overline{\lambda}(\Psi_L) \text{ and } \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L)) \approx \overline{\lambda}(\Psi_L). \tag{91}$$

Using this and (50) we can choose $\mathcal{K}_1$ and a function π_1 such that if $\kappa_L > \mathcal{K}_1$ and $p_{1,L} > \pi_1(\kappa_L)$ then

$$\overline{\lambda}(\Phi_L) > \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L))/2 > (1-\gamma)/2. \tag{92}$$

Set $E''_L = \mathbb{R} \setminus (\overline{\Lambda}'(q_L) \cup \widetilde{\Phi}_L)$, this will be part of the new exceptional set E^L. We also introduce

$$\widetilde{E}''_L = \mathbb{R} \setminus (\overline{\Lambda}'(q_L) \cup \Phi_L) \subset E''_L. \tag{93}$$

It is clear that E''_L is periodic by q_L, while $\widetilde{E}''_L$ is periodic by $\tau'_{L-1} q_L$.

We can choose $\mathcal{K}_2$ and a function π_2 such that if $\kappa_L > \mathcal{K}_2$ and $p_{1,L} > \pi_2(\kappa_L)$ then

$$\overline{\lambda}(\widetilde{E}''_L) \leq \overline{\lambda}(E''_L) < \frac{\delta}{4L'}. \tag{94}$$

Set

$$X_{h,L}(x) = X'_{h,L-1}(x) \text{ if } h \leq K+1 \text{ and } x \in \Phi_L. \tag{95}$$

For $K > 0$ we can make the following comment: Since Φ_L consists of intervals of the form $[j\tau'_{L-1}, (j+1)\tau'_{L-1})$, this definition and the remark after the definition of $X'_{h,L-1}$ in Section 4.2.4 ensures that the functions $X_{h,L}$ are pairwise independent for $h = 1, \ldots, K+1$ and are conditionally M−0.99 distributed on Φ_L for $h = 1, \ldots, K$.

On $\widetilde{E}''_L$ we will have

$$X_{K+1,L}(x) = (1-\rho')\overline{\lambda}(F_{L-1})\widetilde{C}_\gamma \tag{96}$$

and we define $X_{h,L}$ for $h = 1, \ldots, K$ so that they are pairwise independent on $\widetilde{E}''_L$, furthermore, (for $K > 0$) the functions $X_{h,L}$ are conditionally M−0.99-distributed on $\widetilde{E}''_L$ for $h = 1, \ldots, K$. Since $X_{K+1,L}$ is constant on $\widetilde{E}''_L$ it is automatically independent on this set from $X_{h,L}$ for $h = 1, \ldots, K$.

The functions $X_{h,L}$ are periodic on $\widetilde{E}''_L$ by $\tau'_{L-1} q_L$ for $h = 1, \ldots, K+1$. In this way the $X_{h,L}$'s are defined on $\Phi_L \cup \widetilde{E}''_L = \mathbb{R} \setminus \overline{\Lambda}'(q_L)$.

We set $E'_L = \Psi_L \cap {E'}^{L-1}$.

Next we consider some sets which are used to describe the distribution of $X_{K+1,L}$.

If $L=1$ set $S_{1,0}=\mathbb{R}\setminus\overline{\Lambda}'(q_1)$ and $S_{1,1}=\mathbb{R}$.

If $L\geq 2$ first we define $S_{L,l}$ for $l=0,\dots,L-1$ so that $S_{L,l}\cap\Phi_L=S'_{L-1,l}\cap\Phi_L$ for $l=0,\dots,L-1$. We choose $S_{L,l}$ so that $S_{L,l}\cap(\mathbb{R}\setminus\Phi_L)=\varnothing$ for $l=0,\dots,L-2$. We choose $S_{L,L-1}$ so that $S_{L,L-1}=\widetilde{E}''_L\cup(S'_{L-1,L-1}\cap\Phi_L)=\widetilde{E}''_L\cup\Phi_L=\mathbb{R}\setminus\overline{\Lambda}'(q_L)$. Finally, we set $S_{L,L}=\mathbb{R}$, then $S_{L,L}\setminus S_{L,L-1}=\overline{\Lambda}'(q_L)$.

We have by (75), (for the case $L=1$ by (74)) and (95)

$$X_{K+1,L}(x)=(1-\rho')\overline{\lambda}(F_0)\widetilde{C}_\gamma \text{ for } x\in S_{L,0}, \text{ and}$$
$$X_{K+1,L}(x)=(1-\rho')\overline{\lambda}(F_l)\widetilde{C}_\gamma \text{ for } x\in S_{L,l}\setminus S_{L,l-1},\ l=1,\dots,L-1. \tag{97}$$

The case when $l=L$ will be considered in (101). By (93) we have $\widetilde{E}''_L\cap\Phi_L=\varnothing$ and hence $S_{L,l}\cap\widetilde{E}''_L=\varnothing$ for $l\leq L-2$. This implies $\widetilde{E}''_L\subset S_{L,L-1}\setminus S_{L,L-2}$. Hence (97) applied with $l=L-1$ implies (96).

Let $F_L=\Psi_L\cap F'_{L-1}$. Using the fact that F'_{L-1} is periodic by τ'_{L-1} and Ψ_L is the union of some intervals of the form $[j\tau'_{L-1},(j+1)\tau'_{L-1})$ and is periodic by $\tau'_{L-1}q_L$ one can easily see that $\overline{\lambda}(F_L)=\overline{\lambda}(\Psi_L)\overline{\lambda}(F'_{L-1})$. Moreover,

$$r_L\overset{\text{def}}{=}\frac{\overline{\lambda}(F_L)}{\overline{\lambda}(F_{L-1})}=\overline{\lambda}(\Psi_L)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})}\approx\overline{\lambda}(\Psi_L)\approx\overline{\lambda}(\Phi_L)\approx\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_L)).$$

Since $\overline{\lambda}(F'_{L-1})\leq\overline{\lambda}(F_{L-1})$ by (91) there is $\mathcal{K}_3$ and a function π_3 such that if $\kappa_L>\mathcal{K}_3$ and $p_{1,L}>\pi_3(\kappa_L)$, then

$$\overline{\lambda}(\Psi_L)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})}<\frac{1-\gamma}{1-\gamma-\gamma^2}\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_L)). \tag{98}$$

By (51) we obtain

$$\widetilde{C}_\gamma r_L=\widetilde{C}_\gamma\frac{\overline{\lambda}(F_L)}{\overline{\lambda}(F_{L-1})}=\widetilde{C}_\gamma\overline{\lambda}(\Psi_L)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})}<1-\gamma. \tag{99}$$

By (50), (56), (81) and $\overline{\lambda}(\Psi_L)\approx\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_L))$ there is $\mathcal{K}_4$ and a function π_4 such that if $\kappa_L>\mathcal{K}_4$ and $p_{1,L}>\pi_4(\kappa_L)$, then

$$1-2\gamma<r_L=\frac{\overline{\lambda}(F_L)}{\overline{\lambda}(F_{L-1})}=\overline{\lambda}(\Psi_L)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(F_{L-1})}<1-\frac{\gamma}{2}. \tag{100}$$

We set

$$X_{K+1,L}(x)=(1-\rho')\overline{\lambda}(F_L)\widetilde{C}_\gamma \text{ for } x\in S_{L,L}\setminus S_{L,L-1}=\overline{\Lambda}'(q_L). \tag{101}$$

If $L=1$ then $\overline{\lambda}(F_1)=\overline{\lambda}(\Psi_1)\overline{\lambda}(F'_0)\approx\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_1))$ and $\overline{\lambda}(S_{1,0})=\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_1))$. Furthermore, $\overline{\lambda}(S_{1,1})=\overline{\lambda}(\mathbb{R})=1$, $r_1\approx\overline{\lambda}(\mathbb{R}\setminus\overline{\Lambda}'(q_1))$.

By (50), (51), (90) and (91) there is $\mathcal{K}_5$ and a function π_5 such that if $\kappa_1 > \mathcal{K}_5$ and $p_{1,1} > \pi_5(\kappa_1)$, then

$$1 - 1.1\gamma < \overline{\lambda}(\Psi_1) < 1 - \frac{8\gamma}{10} \text{ and } 1 - \rho < \frac{\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_1))}{\overline{\lambda}(\Psi_1)} \leq 1. \tag{102}$$

From (80), (81), (91) and (102) it follows that

(103)

$$\begin{aligned} &1 - 2\gamma < r_1 = \overline{\lambda}(\Psi_1)\frac{\overline{\lambda}(F_0')}{\overline{\lambda}(F_0)} < 1 - \frac{\gamma}{2}, \\ &\frac{1}{1-\rho}\overline{\lambda}(F_1) = \frac{1}{1-\rho}\overline{\lambda}(\Psi_1)\overline{\lambda}(F_0') \\ &\qquad > \overline{\lambda}(S_{1,0}) = \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_1)) > (1-\rho)\overline{\lambda}(\Psi_1)\overline{\lambda}(F_0') = (1-\rho)\overline{\lambda}(F_1), \end{aligned}$$

(keeping in mind $F_0 = \mathbb{R}$)

(104)

$$\begin{aligned} \frac{1}{(1-\rho)r_0 r_1}\overline{\lambda}(S_{1,0}) &= \frac{\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_1))\overline{\lambda}(F_0)}{(1-\rho)\overline{\lambda}(\Psi_1)\overline{\lambda}(F_0')} > \overline{\lambda}(S_{1,1}) = 1 \\ &> (1-\rho)\frac{\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_1))\overline{\lambda}(F_0)}{\overline{\lambda}(\Psi_1)\overline{\lambda}(F_0')} = (1-\rho)\frac{1}{r_0 r_1}\overline{\lambda}(S_{1,0}) \end{aligned}$$

and

$$\frac{1}{1-\rho}\overline{\lambda}(S_{1,0}) > \overline{\lambda}(F_1)\overline{\lambda}(S_{1,1}) > (1-\rho)\overline{\lambda}(S_{1,0}). \tag{105}$$

This shows that (109) and (110) below hold for $L = 1$ and $l = 1$. For $L = 1$ and $l = 0$, (109) and (110) are obvious.

If $L \geq 2$ we have $\overline{\lambda}(S_{L,0}) = \overline{\lambda}(\Phi_L) \cdot \overline{\lambda}(S'_{L-1,0})$. From (82) it follows that

$$1 > (1-\rho)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(S'_{L-1,0})}. \tag{106}$$

Therefore, by (90) and (91) there is $\mathcal{K}_6$ and a function π_6 such that if $\kappa_L > \mathcal{K}_6$ and $p_{1,L} > \pi_6(\kappa_L)$ then

$$1 \geq \frac{\overline{\lambda}(\Phi_L)}{\overline{\lambda}(\Psi_L)} > (1-\rho)\frac{\overline{\lambda}(F'_{L-1})}{\overline{\lambda}(S'_{L-1,0})}. \tag{107}$$

Using this, (82) and (91) a simple calculation shows that

$$\begin{aligned} \frac{1}{1-\rho}\overline{\lambda}(F_L) &= \frac{1}{1-\rho}\overline{\lambda}(\Psi_L)\overline{\lambda}(F'_{L-1}) > \overline{\lambda}(S_{L,0}) = \overline{\lambda}(\Phi_L)\overline{\lambda}(S'_{L-1,0}) \\ &> (1-\rho)\overline{\lambda}(\Psi_L)\overline{\lambda}(F'_{L-1}) = (1-\rho)\overline{\lambda}(F_L). \end{aligned} \tag{108}$$

It is also clear that $\overline{\lambda}(S_{L,l}) = \overline{\lambda}(\Phi_L) \cdot \overline{\lambda}(S'_{L-1,l})$ for $l = 0, \dots, L-2$. Using (77) we have for $l = 0, \dots, L-2$

$$\frac{1}{(1-\rho) r_0 \cdots r_l} \overline{\lambda}(S_{L,0}) > \overline{\lambda}(S_{L,l}) > (1-\rho) \frac{1}{r_0 \cdots r_l} \overline{\lambda}(S_{L,0}) \tag{109}$$

and by $\overline{\lambda}(F_l) = r_0 \cdots r_l$, we have

$$\frac{1}{1-\rho} \overline{\lambda}(S_{L,0}) > \overline{\lambda}(F_l) \overline{\lambda}(S_{L,l}) > (1-\rho) \overline{\lambda}(S_{L,0}). \tag{110}$$

When $l = L-1$ a little caution is needed. We have $\overline{\lambda}(S_{L,L-1}) = (\overline{\lambda}(\Phi_L) + \overline{\lambda}(\widetilde{E}''_L)) \overline{\lambda}(S'_{L-1,L-1}) = \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L))$. By (77),

$$\frac{1}{(1-\rho) r_0 \cdots r_{L-1}} \cdot \frac{\overline{\lambda}(S'_{L-1,0})}{\overline{\lambda}(S'_{L-1,L-1})} > 1.$$

Hence, there is $\mathcal{K}_7 \geq \mathcal{K}_1$ and a function $\pi_7 \geq \pi_1$ such that if $\kappa_L > \mathcal{K}_7$ and $p_{1,L} > \pi_7(\kappa_L)$, then using (92) and (94),

$$\begin{aligned} \frac{1}{(1-\rho) r_0 \cdots r_{L-1}} \cdot \frac{\overline{\lambda}(S'_{L-1,0})}{\overline{\lambda}(S'_{L-1,L-1})} &> 1 + \frac{2\overline{\lambda}(E''_L)}{1-\gamma} \\ &> 1 + \frac{\overline{\lambda}(\widetilde{E}''_L)}{\overline{\lambda}(\Phi_L)} = \frac{\overline{\lambda}(\Phi_L) + \overline{\lambda}(\widetilde{E}''_L)}{\overline{\lambda}(\Phi_L)}. \end{aligned} \tag{111}$$

Using this and (77) one can deduce that (109) and (110) hold when $l = L-1$.

From $\overline{\lambda}(S_{L,L}) = 1$ and (108) it follows that

$$\frac{1}{1-\rho} \overline{\lambda}(S_{L,0}) > \overline{\lambda}(F_L) \overline{\lambda}(S_{L,L}) > (1-\rho) \overline{\lambda}(S_{L,0}).$$

Using the fact that $\overline{\lambda}(F_L) = r_0 \cdots r_L$ we find that (109) and (110) hold for $l = L$ as well.

Denote by $\overline{E}'''_L$ the set of those n's for which

$$\#\Big(((n + \Lambda_0(q_L)) \setminus \Lambda(q_L)) \cap [0, q_L) \Big) < (1-\widetilde{\rho})(1-\gamma) \#(\Lambda_0(q_L) \cap [0, q_L)). \tag{112}$$

Recall that by our choice $p_{1,L} > p'_{1,L}$ and hence q_L satisfies (14) with $\epsilon = \delta/4L'$ and $\widetilde{\rho}$ instead of ρ. Lemma 2 yields

$$\#(\overline{E}'''_L \cap [0, q_L)) < \frac{\delta}{4L'} q_L. \tag{113}$$

Set

$$E'''_L = \{x \in \mathbb{R} : \lfloor x \rfloor \in \overline{E}'''_L\}. \tag{114}$$

Then $\overline{\lambda}(E_L''') < \delta/4L'$ and if $x \notin E_L'''$ we have

$$\begin{aligned}(115)\quad &\frac{1}{q_L}\#\{k' \in [0,q_L)\cap\mathbb{Z} : \lfloor x\rfloor + k'^2 \notin \Lambda(q_L)\}\\ &\geq \frac{1}{q_L}\#\{k' \in [0,q_L)\cap\mathbb{Z} : \lfloor x\rfloor + k'^2 \notin \Lambda(q_L), k'^2 \in \Lambda_0'(q_L)\}\\ &\geq \frac{1}{q_L}2^{\kappa_L}\#(((\lfloor x\rfloor + \Lambda_0'(q_L))\setminus\Lambda(q_L))\cap[0,q_L))\\ &\geq \frac{1}{q_L}2^{\kappa_L}\Big(\#(((\lfloor x\rfloor + \Lambda_0(q_L))\setminus\Lambda(q_L))\cap[0,q_L))\\ &\qquad -\#((\Lambda_0(q_L)\setminus\Lambda_0'(q_L))\cap[0,q_L))\Big)\end{aligned}$$

(using that for $\lfloor x\rfloor \notin \overline{E}_L'''$ we have the negation of (112))

$$\begin{aligned}&\geq \frac{1}{q_L}2^{\kappa_L}\Big(((1-\widetilde{\rho})(1-\gamma)\#(\Lambda_0(q_L)\cap[0,q_L)))\\ &\qquad -\#((\Lambda_0(q_L)\setminus\Lambda_0'(q_L))\cap[0,q_L))\Big) = (*).\end{aligned}$$

Recall that we assumed that $p_{1,L} > \pi_0(\kappa_L)$. Thus we can apply (85) yielding

$$(*) \geq \frac{1}{q_L}2^{\kappa_L}(1-2\widetilde{\rho})(1-\gamma)\#(\Lambda_0(q_L)\cap[0,q_L)) = (**).$$

Using (3) we can finish with the inequality

$$(116)\qquad (**) > \frac{1}{q_L}2^{\kappa_L}(1-2\widetilde{\rho})(1-\gamma)\frac{q_L}{2^{\kappa_L}} = (1-2\widetilde{\rho})(1-\gamma).$$

4.2.6. *Putting $K - M$ families on $\overline{\Lambda}'(q_L)$.* In this section we check the domination property of averages along squares for one part of the complement of E^L.

We put

$$(117)\qquad f_{K+1,L} = f'_{K+1,L-1}\cdot\chi_{\Psi_L}.$$

Then indeed, $F_L = \{x : f_{K+1,L}(x) = 1\} = \Psi_L \cap F'_{L-1}$, and we have $\overline{\int} f_{K+1,L} = \overline{\lambda}(F_L)$. Since $f'_{K+1,L-1}$ is periodic by $\tau'_{L-1} \in \mathcal{P}'_{L-1}$ and Ψ_L is periodic by $\tau'_{L-1}q_L$ the function $f_{K+1,L}$ is also periodic by $\tau'_{L-1}q_L$.

When $K > 0$ and $h \in \{1,\ldots,K\}$ we will define $f_{h,L}$ in (135) so that

$$f_{h,L}(x) = f'_{h,L-1}(x) \text{ for } x \in \Phi_L.$$

Choose $\mathcal{P}''_L \subset \mathcal{P}'_L$ such that it contains infinitely many primes and all their possible products, moreover all numbers in $\mathcal{P}''_L$ are relatively prime to $q_L \in \mathcal{P}'_L$ and set $\overline{\mathcal{P}}_L = \mathcal{P}\cup\mathcal{P}''_L\cup\mathcal{P}'_{L+1}\cup\cdots\cup\mathcal{P}'_{L'}$.

When $K=0$, *i.e.*, when constructing a $1-M$ family we have to put a vacuous "$0-M$ family" on $\overline{\Lambda}'(q_L)$.

Hence, for $K=0$, for the definition of a $1-M$ family we just set $\overline{\tau}_L = q_L(\tau'_{L-1})^3$, $E_{\delta_L}=\varnothing$.

When $K\geq 1$ this step is crucial, see Section 4.2.13.

Set $\mathcal{P}_L=\mathcal{P}\cup\mathcal{P}'_{L+1}\cup\cdots\cup\mathcal{P}'_{L'}\subset\overline{\mathcal{P}}_L\subset\mathcal{P}_{L-1}$. We also put $E^L=E_{\delta_L}\cup E'_L\cup E''_L\cup E'''_L$, and $\tau_L=q_L\overline{\tau}_L\tau'_{L-1}$. When $K=0$ we defined $\overline{\tau}_L=q_L(\tau'_{L-1})^3$ and hence $\tau_L=q_L^2(\tau'_{L-1})^4$. Then for all $p\in\mathcal{P}_L\subset\overline{\mathcal{P}}_L$ we have $(\tau_L,p)=1$ and $(\tau'_{L-1}(x),p)=1$ when $x\in\mathbb{R}\setminus E^L$. Assume $x\in\mathbb{R}\setminus(\overline{\Lambda}'(q_L)\cup E^L)$. Then $x\in\widetilde{\Phi}_L\subset\Phi_L$ and the old estimates work.

In other words, for $x\in\mathbb{R}\setminus(\overline{\Lambda}'(q_L)\cup E^L)\subset\widetilde{\Phi}_L$, set $\alpha_L(x)=\alpha'_{L-1}(x)$, $\omega_L(x)=\omega'_{L-1}(x)$, $\tau_L(x)=\tau'_{L-1}(x)=\tau_{L-1}(x)$. Then $\omega_L^2(x)<\tau_{L-1}<\tau'_{L-1}<\tau_L$ and by (83) we have

$$\frac{\omega'_{L-1}(x)}{\alpha'_{L-1}(x)}=\frac{\omega_L(x)}{\alpha_L(x)}>\Omega\tau'_{L-1}(x)=\Omega\tau_L(x).$$

Observe that if $x\in\mathbb{R}\setminus(\overline{\Lambda}'(q_L)\cup E^L)\subset\widetilde{\Phi}_L\setminus E'_L=\widetilde{\Phi}_L\setminus E'^{L-1}\subset\widetilde{\Phi}_L\subset\Phi_L$, then from $x\notin E'^{L-1}$, $\alpha_L(x)\leq n\leq k<n+m\leq\omega_L(x)$, and $\omega_L^2(x)<\tau_{L-1}<\tau'_{L-1}$ it follows that $x+k^2\in\Phi_L\subset\Psi_L$ and hence by (117), $f_{K+1,L}(x+k^2)=f'_{K+1,L-1}(x+k^2)$ and by (84) , if $\tau_L(x)=\tau'_{L-1}(x)|m$, then

$$\begin{aligned}\frac{1}{m}\sum_{k=n}^{n+m-1}f'_{K+1,L-1}(x+k^2)&=\frac{1}{m}\sum_{k=n}^{n+m-1}f_{K+1,L}(x+k^2)\\&>X_{K+1,L}(x)=X'_{K+1,L-1}(x).\end{aligned}$$

Finally, for all $x\in\mathbb{R}\setminus(\overline{\Lambda}'(q_L)\cup E^L)\subset\widetilde{\Phi}_L\setminus E'_L=\widetilde{\Phi}_L\setminus E'^{L-1}\subset\widetilde{\Phi}_L$, $h=1,\dots,K+1$, if $\alpha_L^2(x)\leq j<j+\tau_L(x)\leq\omega_L^2(x)<\tau_{L-1}$, then $x+j$, $x+j+\tau_L(x)\in\Phi_L$ and

$$f'_{h,L-1}(x+j+\tau'_{L-1}(x))=f_{h,L}(x+j+\tau_L(x))=f_{h,L}(x+j)=f'_{h,L-1}(x+j).$$

†Assume $x\in\overline{\Lambda}'(q_L)\setminus E^L\subset\overline{\Lambda}'(q_L)\setminus E_{\delta_L}$.

For the $K=0$ case set $\alpha_L(x)=\alpha'_{L-1}(x)$, $\omega_L(x)=\tau'_{L-1}q_L\omega'_{L-1}(x)$, and $\tau_L(x)=\tau'_{L-1}q_L\tau'_{L-1}(x)$. Then $\omega_L^2(x)<(\tau'_{L-1})^2q_L^2(\tau'_{L-1})^2=\tau_L$ and

$$\frac{\omega_L(x)}{\alpha_L(x)}=\frac{\omega'_{L-1}(x)\tau'_{L-1}q_L}{\alpha'_{L-1}(x)}>\Omega\tau'_{L-1}(x)\tau'_{L-1}q_L=\Omega\tau_L(x).$$

Since $f_{K+1,L}$ is periodic by $\tau'_{L-1}q_L$ and $\tau'_{L-1}q_L|\tau_L(x)$ we have $f_{K+1,L}(x+j+\tau_L(x))=f_{K+1,L}(x+j)$ for all x and j.

Instead of the above paragraph we will have a different argument in Section 4.2.13 for the $K>0$ case.

4.2.7. *Properties of $f_{K+1,L}$.* In this section we check the domination property for averages along squares for x in the remaining part of the complement of E^L.

We need to check (64) when $h = K+1$ and

$$x \in \overline{\Lambda}'(q_L) \setminus E^L = (S_{L,L} \setminus S_{L,L-1}) \setminus E^L, \text{ and } \tau_L(x) = \tau'_{L-1} q_L \tau'_{L-1}(x)|m.$$

If we can show that (64) holds when $m = \tau'_{L-1} q_L$ then this clearly implies that it holds when $\tau_L(x)|m$. Recall that $\widehat{\Psi}_L$ is periodic by q_L. Since $\tau'_{L-1} \in \mathcal{P}'_{L-1}$, $q_L \in \mathcal{P}'_L$ implies $(\tau'_{L-1}, q_L) = 1$, $k' + jq_L$ covers all residues modulo τ'_{L-1} as j runs from 0 to $\tau'_{L-1} - 1$. Since $f'_{K+1,L-1}$ is periodic by τ'_{L-1}, using (79) we obtain

$$\frac{1}{\tau'_{L-1}} \sum_{j=0}^{\tau'_{L-1}-1} f'_{K+1,L-1}(x + (k' + jq_L)^2) > \left(1 - \frac{\rho'}{2}\right) \overline{\lambda}(F_{L-1}). \tag{118}$$

Also observe that from the periodicity of $\widehat{\Psi}_L$ by q_L it follows that if $x + k'^2 \in \widehat{\Psi}_L$ then $x + (k' + jq_L)^2 \in \widehat{\Psi}_L \subset \Psi_L$ as well. Hence from $x + k'^2 \in \widehat{\Psi}_L$ it follows that $f_{K+1,L}(x + (k' + jq_L)^2) = f'_{K+1,L-1}(x + (k' + jq_L)^2)$. Therefore,

$$\begin{aligned}
&\frac{1}{\tau'_{L-1} q_L} \sum_{k=n}^{n+\tau'_{L-1} q_L - 1} f_{K+1,L}(x + k^2) \\
&= \frac{1}{\tau'_{L-1} q_L} \sum_{k'=n}^{n+q_L-1} \sum_{j=0}^{\tau'_{L-1}-1} f_{K+1,L}(x + (k' + jq_L)^2) \\
&\geq \frac{1}{\tau'_{L-1} q_L} \sum_{\substack{k'=n \\ x+k'^2 \in \widehat{\Psi}_L}}^{n+q_L-1} \sum_{j=0}^{\tau'_{L-1}-1} f_{K+1,L}(x + (k' + jq_L)^2) \\
&= \frac{1}{q_L} \sum_{\substack{k'=n \\ x+k'^2 \in \widehat{\Psi}_L}}^{n+q_L-1} \frac{1}{\tau'_{L-1}} \sum_{j=0}^{\tau'_{L-1}-1} f'_{K+1,L-1}(x + (k' + jq_L)^2)
\end{aligned}$$

(using (118))

$$> \frac{1}{q_L} \sum_{\substack{k'=n \\ x+k'^2 \in \widehat{\Psi}_L}}^{n+q_L-1} \left(1 - \frac{\rho'}{2}\right) \overline{\lambda}(F_{L-1})$$

(using (88))

$$\geq \frac{1}{q_L}\left(1-\frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1})\#\{k'\in[0,q_L)\cap\mathbb{Z}: x+k'^2\notin\overline{\Lambda}'(q_L)\}$$
$$\geq \frac{1}{q_L}\left(1-\frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1})\#\{k'\in[0,q_L)\cap\mathbb{Z}: x+k'^2\notin\overline{\Lambda}(q_L)\}$$
$$=\left(1-\frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1})\frac{1}{q_L}\#\{k'\in[0,q_L)\cap\mathbb{Z}: \lfloor x\rfloor+k'^2\notin\Lambda(q_L)\}.$$

Now use the estimates (115) through (116) and obtain that for $x\notin E_L'''\subset E^L$

$$\frac{1}{q_L}\#\{k'\in[0,q_L)\cap\mathbb{Z}: \lfloor x\rfloor+k'^2\notin\Lambda(q_L)\}\geq(1-2\widetilde{\rho})(1-\gamma).$$

Thus, if $x\in(S_{L,L}\setminus S_{L,L-1})\setminus E^L=\overline{\Lambda}'(q_L)\setminus E^L$ we have

$$\frac{1}{\tau'_{L-1}q_L}\sum_{k=n}^{n+\tau'_{L-1}q_L-1} f_{K+1,L}(x+k^2)$$
$$>\left(1-\frac{\rho'}{2}\right)\overline{\lambda}(F_{L-1})(1-2\widetilde{\rho})(1-\gamma)$$

(using (62), (99) and (101))

$$\geq(1-\rho')(1-\gamma)\overline{\lambda}(F_{L-1})>(1-\rho')\widetilde{C}_\gamma\overline{\lambda}(F_L)=X_{K+1,L}(x).$$

4.2.8. *Finishing the leakage.* We keep repeating the leakage steps until for the first time for some L'' we have $\overline{\lambda}(F_{L''})<2^{-M}$ which implies $\overline{\lambda}(F_{L''-1})\geq 2^{-M}$. By (57) and (100) applied to all $L\leq L'$ we have $L''\leq L'$ and by $\gamma<\gamma_0<10^{-7}$ we have $L''\geq 2$.

We set $f_h=f_{h,L''}$ for $h=1,\dots,K+1$, and $X_h=X_{h,L''}$ for $h=1,\dots,K$. From the induction steps we have $E_\delta\overset{\text{def}}{=}E^{L''}$ such that $\overline{\lambda}(E_\delta)<\frac{(L''+1)}{(L'+1)}\delta\leq\delta$. There exists $\tau\overset{\text{def}}{=}\tau_{L''}$ such that f_h, $h=1,\dots,K+1$, X_h, $h=1,\dots,K$ and $X_{K+1,L''}$ are periodic by τ, X_h, $h=1,\dots,K$ and $X_{K+1,L''}$ are pairwise independent X_h, $h=1,\dots,K$ are $M-0.99$-distributed. By using the distributional properties of $X_{K+1,L''}$ we will define X_{K+1} at the end of this section.

For all $x\notin E_\delta$ there exist $\omega(x)=\omega_{L''}(x)>\alpha(x)=\alpha_{L''}(x)>A$, $\tau(x)=\tau_{L''}(x)<\tau$ such that $\omega^2(x)<\tau$, $\frac{\omega(x)}{\alpha(x)}>\Omega\tau(x)$. Setting $f_{K+1}=f_{K+1,L''}$ (see also (117)), if $\tau(x)|m$ then

$$\frac{1}{m}\sum_{k=n}^{n+m-1} f_{K+1}(x+k^2)>X_{K+1,L''}(x). \tag{119}$$

When $K>0$ one also needs to use (139); see Section 4.2.15.

For all $p \in \mathcal{P}_{L''} \supset \mathcal{P}$, $(\tau(x), p) = 1$, $(\tau, p) = 1$. For all $x \notin E_\delta$ and for all $h \in \{1, \dots, K+1\}$, $f_h(x + j + \tau(x)) = f_h(x + j)$ whenever $\alpha^2(x) \le j < j + \tau(x) \le \omega^2(x)$. Finally,

$$\overline{\int} f_{K+1} = \overline{\lambda}(F_{L''}) < 2^{-M+1} < \Gamma \cdot 2^{-M+1}, \tag{120}$$

when $K > 0$ we also need (140) from Section 4.2.15.

We have met all the requirements for a $(K+1)-M$ family except the distribution of $X_{K+1,L''}$ is not quite right. We need to replace $X_{K+1,L''}$ by a suitably chosen X_{K+1} which is $M-0.99$-distributed, moreover for $K > 0$ it is pairwise independent from X_h when $h = 1, \dots, K$. By choosing X_{K+1} so that $X_{K+1} \le X_{K+1,L''}$ from (119) we infer that if $\alpha(x) \le n < n + m \le \omega(x)$ and $\tau(x)|m$, then

$$\frac{1}{m} \sum_{k=n}^{n+m-1} f_{K+1}(x + k^2) > X_{K+1}(x). \tag{121}$$

Since L'' is the first index when $\overline{\lambda}(F_{L''}) < 2^{-M}$ we have $\overline{\lambda}(F_{L''-1}) \ge 2^{-M}$ which by (100) implies

$$\overline{\lambda}(F_{L''}) > (1 - 2\gamma) 2^{-M}. \tag{122}$$

What is the distribution of $X_{K+1,L''}$? Recall $F_{L''} = \{x : f_{K+1}(x) = 1\}$, $1 - 2\gamma < r_L = \overline{\lambda}(F_L)/\overline{\lambda}(F_{L-1}) < 1 - \frac{\gamma}{2}$, for $L = 1, \dots, L''$, and $\overline{\lambda}(F_L) = r_0 \cdots r_L = r_1 \cdots r_L$. By (108) and (59)

$$\frac{1}{1-\rho} 2^{-M} > \frac{1}{1-\rho} \overline{\lambda}(F_{L''}) > \overline{\lambda}(S_{L'',0}) > (1-\rho) \overline{\lambda}(F_{L''}) > (1 - 3\gamma) 2^{-M}. \tag{123}$$

By (97), $X_{K+1,L''}(x) = (1 - \rho') \widetilde{C}_\gamma \cdot 1 = (1 - \rho') \widetilde{C}_\gamma \overline{\lambda}(F_0)$ if $x \in S_{L'',0}$.

By (97) and (101) if $x \in S_{L'',l} \setminus S_{L'',l-1}$ then for $l = 1, \dots, L''$,

$$X_{K+1,L''}(x) = (1 - \rho') r_0 \cdots r_l \widetilde{C}_\gamma = (1 - \rho') \overline{\lambda}(F_l) \widetilde{C}_\gamma. \tag{124}$$

This and (60) imply that for $x \in S_{L'',L''} \setminus S_{L'',L''-1}$

$$X_{K+1,L''}(x) = (1 - \rho') \widetilde{C}_\gamma \overline{\lambda}(F_{L''}) < 2^{-M} (1 - \rho') \widetilde{C}_\gamma < 0.999 \cdot 2^{-M+1}. \tag{125}$$

Using (109) we have the following measure estimate:

$$\frac{1}{(1-\rho) r_0 \cdots r_l} \overline{\lambda}(S_{L'',0}) > \overline{\lambda}(S_{L'',l}) > (1-\rho) \frac{1}{r_0 \cdots r_l} \overline{\lambda}(S_{L'',0}),$$

which by (110) is equivalent to

$$\frac{1}{1-\rho} \overline{\lambda}(S_{L'',0}) > \overline{\lambda}(F_l) \overline{\lambda}(S_{L'',l}) > (1-\rho) \overline{\lambda}(S_{L'',0}). \tag{126}$$

Suppose for $l = 0, \dots, M-1$, $\ell'(l)$ is chosen so that

$$X_{K+1,L''}(x) \geq 0.999 \cdot 2^{-l} \text{ when } x \in S_{L'',\ell'(l)}, \tag{127}$$

but $X_{K+1,L''}(x) < 0.999 \cdot 2^{-l}$ for some $x \in S_{L'',\ell'(l)+1}$, by (125) such an $\ell'(l) \leq L''$ exists. By (124)

$$(1-\rho')\overline{\lambda}(F_{\ell'(l)+1})\widetilde{C}_\gamma < 0.999 \cdot 2^{-l},$$

and

$$(1-\rho')\overline{\lambda}(F_{\ell'(l)})\widetilde{C}_\gamma \geq 0.999 \cdot 2^{-l}$$

hold. Therefore, using $\overline{\lambda}(F_{\ell'(l)+1})/\overline{\lambda}(F_{\ell'(l)}) > (1-2\gamma)$ we infer

$$0.999 \cdot 2^{-l} \leq (1-\rho')\overline{\lambda}(F_{\ell'(l)})\widetilde{C}_\gamma < \frac{0.999}{1-2\gamma}2^{-l}. \tag{128}$$

Set $S_{L'',\ell'(-1)} = \varnothing$. By using (124) and the above definitions, estimates for $l = 0, \dots, M-1$, $x \in S_{L'',\ell'(l)} \setminus S_{L'',\ell'(l-1)}$ we have

$$0.999 \cdot 2^{-l} \leq X_{K+1,L''}(x) < 0.999 \cdot 2^{-(l-1)}. \tag{129}$$

By (126)

$$\overline{\lambda}(S_{L'',\ell'(l)}) < \frac{1}{1-\rho}\overline{\lambda}(S_{L'',0})\frac{1}{\overline{\lambda}(F_{\ell'(l)})}$$

(using (123) and (128))

$$< \frac{1}{(1-\rho)^2}\overline{\lambda}(F_{L''})\frac{(1-\rho')\widetilde{C}_\gamma}{0.999 \cdot 2^{-l}} < \frac{(1-\rho')\widetilde{C}_\gamma 2^l}{0.999 \cdot (1-\rho)^2}2^{-M},$$

on the other hand, by using (126)

$$\overline{\lambda}(S_{L'',\ell'(l)}) > \frac{(1-\rho)\overline{\lambda}(S_{L'',0})}{\overline{\lambda}(F_{\ell'(l)})}$$

(using (123) and (128) again)

$$> \frac{(1-\rho)^2\overline{\lambda}(F_{L''})(1-\rho')\widetilde{C}_\gamma(1-2\gamma)}{0.999 \cdot 2^{-l}}$$

(using (122))

$$> (1-\rho)^2(1-2\gamma)^2 2^{-M} \cdot 2^l(1-\rho')\widetilde{C}_\gamma.$$

Thus using (61) for $l = 0, \dots, M-1$

$$\begin{aligned} &\overline{\lambda}(S_{L'',\ell'(l)} \setminus S_{L'',\ell'(l-1)}) \\ &> (1-\rho)^2(1-2\gamma)^2 2^{-M+l}(1-\rho')\widetilde{C}_\gamma - \frac{(1-\rho')\widetilde{C}_\gamma}{0.999 \cdot (1-\rho)^2} \cdot 2^{-M+l-1} \\ &> 0.99 \cdot 2^{-M+l-1}. \end{aligned} \tag{130}$$

By (129) if $l = 0, \dots, M-1$, $x \in S_{L'',\ell'(l)} \setminus S_{L'',\ell'(l-1)}$ we have $X_{K+1,L''}(x) \geq 0.999 \cdot 2^{-l}$.

By (124), $X_{K+1,L''}$ takes different constant values on the set $S_{L'',0}$ and on the sets $S_{L'',l} \setminus S_{L'',l-1}$ for $l = 1, \dots, L''$.

When $K > 0$ we also know that $X_{K+1,L''}$ is pairwise independent from X_h for $h = 1, \dots, K$. Hence, any function which is constant on the sets $S_{L'',0}$, $S_{L'',l} \setminus S_{L'',l-1}$, $l = 1, \dots, L''$ is still independent from each X_h for $h = 1, \dots, K$.

Set $X'_{K+1}(x) = 0.99 \cdot 2^{-l}$ if $x \in S_{L'',\ell'(l)} \setminus S_{L'',\ell'(l-1)}$ for $l = 0, \dots, M-1$. Set $X'_{K+1}(x) = 0$ if $x \notin S_{L'',\ell'(M-1)}$. Now $X'_{K+1} \leq X_{K+1,L''}$. When $K > 0$, X'_{K+1} is still independent from each X_h, $h = 1, \dots, K$ and it takes its values in $\{0, 0.99, \dots, 0.99 \cdot 2^{-M+1}\}$. But it is M−0.99 super distributed. By Lemma 4 we can choose an M−0.99-distributed $X_{K+1} \leq X'_{K+1}$ which is still independent from X_h for each $h = 1, \dots, K$. This completes the part of our proof when we build the $1-M$ family, that is for $K = 0$ our argument ends here.

4.2.9. *The $K > 0$ cases of our induction Step. $L = 0$ of our leakage.* Next we assume that $K \geq 1$ and we can define $K - M$ families.

We use the definitions of the first paragraph of Section 4.2.2. After the definition of $X_{K+1,0}$ we argue this way:

Choose a $K - M$ family on $\mathbb{R}$ with input constants $\delta_0 = \frac{\delta}{4(L'+1)}$, $\Omega_0 = \Omega$, $\Gamma_0 C_\gamma < \Gamma$, $A_0 = A$, $\mathcal{P}_0$. Then there exist a period τ_0; functions $f_{h,0} : \mathbb{R} \to [0, \infty)$, pairwise independent M−0.99-distributed "random" variables $X_{h,0} : \mathbb{R} \to \mathbb{R}$, for $h = 1, \dots, K$, a set E_{δ_0} periodic by τ_0, with $\overline{\lambda}(E_{\delta_0}) < \delta_0$. Moreover, for all $x \notin E_{\delta_0}$, there exist $\omega_0(x) > \alpha_0(x) > A$, $\tau_0(x) < \tau_0$ such that $\omega_0^2(x) < \tau_0$, $\frac{\omega_0(x)}{\alpha_0(x)} > \Omega \tau_0(x) = \Omega_0 \tau_0(x)$, if $\alpha_0(x) \leq n < n + m \leq \omega_0(x)$, and $\tau_0(x) | m$ then for all $h = 1, \dots, K+1$ (for $h = 1, \dots, K$ by the definition of the $K - M$ family, for $h = K+1$ by the definition in the first line of Section 4.2.2) there exists $0 \leq f_{h,0}$ such that

$$\frac{1}{m} \sum_{k=n}^{n+m-1} f_{h,0}(x + k^2) > X_{h,0}(x).$$

For all $p \in \mathcal{P}_0$, $(\tau_0(x), p) = 1$, $(\tau_0, p) = 1$. For all $x \notin E_{\delta_0}$ and all $h = 1, \dots, K+1$, $f_{h,0}(x + j + \tau_0(x)) = f_{h,0}(x + j)$ whenever $\alpha_0^2(x) \leq j < j + \tau_0(x) \leq \omega_0^2(x)$. Finally,

$$\frac{1}{\tau_0} \int_0^{\tau_0} f_{h,0} = \overline{\int} f_{h,0} < C_\gamma \Gamma_0 \cdot 2^{-M+1},$$

for $h = 1, \dots, K$.

4.2.10. *Case $K > 0$, the setting after step $L - 1$ of the leakage.* We can repeat almost exactly the argument of Section 4.2.3. We only need to add after the paragraph ending with (64) that for $h = 1, \dots, K$

$$\frac{1}{\tau_{L-1}} \int_0^{\tau_{L-1}} f_{h,L-1} = \overline{\int} f_{h,L-1} < C_\gamma \Gamma_0 \cdot 2^{-M+1}. \tag{131}$$

We emphasize that we do not expect that (131) holds for $h = K + 1$ and continue with the paragraphs of Section 4.2.3 concerning the distribution of $X_{K+1,L-1}$.

4.2.11. *Case* $K > 0$, *rearrangement with respect to* τ'_{L-1}, *choice of* τ'_{L-1}. This subsection is again almost completely identical to Section 4.2.4. The only extra remark we need after the first line of the last paragraph of Section 4.2.4 is the following: We also have

$$\overline{\int} f'_{h,L-1} \leq \overline{\int} f_{h,L-1} < C_\gamma \Gamma_0 \cdot 2^{-M+1}, \tag{132}$$

for $h = 1, \dots, K$.

4.2.12. *Case* $K > 0$, *choice of* κ_L, q_L, Φ_L, Ψ_L, *and* $X_{h,L}$ *on* $\mathbb{R} \setminus \overline{\Lambda}'(q_L)$. This subsection is identical to Section 4.2.5.

4.2.13. *Case* $K > 0$, *putting* $K - M$ *families on* $\overline{\Lambda}'(q_L)$. This is the subsection where we have a huge difference. This is where we need to use the results from the previous step of the induction on K.

The first four paragraphs until the definition of $\overline{\mathcal{P}}_L$ are identical to the ones in Section 4.2.6.

Contrary to the $K = 0$ case now we have to put a $K - M$ family on $\overline{\Lambda}'(q_L)$.

For the choice of the $K - M$ family living on $\overline{\Lambda}'(q_L)$ use Lemma 6 with $\overline{\mathcal{P}}_L$, $\delta_L = \delta/4(L' + 1)$, $\Omega_L = \Omega \cdot q_L \tau'_{L-1}$, Γ_0 and A.

(i) We obtain functions $\overline{f}_{h,L}$, $\overline{X}_{h,L}$ periodic by $\overline{\tau}_L q_L$ for $h = 1, \dots, K$, where $\overline{\tau}_L$ is a suitable natural number. The functions $\overline{X}_{h,L} : \mathbb{R} \to \mathbb{R}$ are pairwise independent and conditionally M–0.99 distributed on $\overline{\Lambda}'(q_L)$. There exists E_{δ_L} periodic by $\overline{\tau}_L q_L$. For $h = 1, \dots, K$ and $x \notin \overline{\Xi}(q_L) = \cup_{j \in \mathbb{Z}} [j q_L, j q_L + \gamma 2^{\kappa_L})$ we have $\overline{f}_{h,L}(x) = 0$.

(ii) We have $\overline{\lambda}(E_{\delta_L}) < \delta_L = \delta/4(L' + 1)$. For all $x \notin E_{\delta_L}$, there exist $\overline{\omega}_L(x) > \overline{\alpha}_L(x) > A$, $\overline{\tau}_L(x) < \overline{\tau}_L q_L$, $\overline{\omega}^2_L(x) < \overline{\tau}_L q_L$,

$$\frac{\overline{\omega}_L(x)}{\overline{\alpha}_L(x)} > \Omega_L \overline{\tau}_L(x) = \Omega q_L \tau'_{L-1} \overline{\tau}_L(x).$$

Moreover, if $\overline{\alpha}_L(x) \leq n < n + m \leq \overline{\omega}_L(x)$ and $\overline{\tau}_L(x) | m$ then for $h = 1, \dots, K$,

$$\frac{1}{m} \sum_{k=n}^{n+m-1} \overline{f}_{h,L}(x + k^2) > \overline{X}_{h,L}(x). \tag{133}$$

(iii) For all $p \in \overline{\mathcal{P}}_L$, $(\overline{\tau}_L(x), p) = 1$, $(\overline{\tau}_L q_L, p) = 1$.

(iv) For all $x \in \overline{\Lambda}'(q_L) \setminus E_{\delta_L}$, for all $h = 1, \dots, K$,

$$\overline{f}_{h,L}(x + j + \overline{\tau}_L(x)) = \overline{f}_{h,L}(x + j),$$

when $\overline{\alpha}_L^2(x) \leq j < j + \overline{\tau}_L(x) \leq \overline{\omega}_L^2(x)$.

(v) Finally, for all $h = 1, \dots, K$

$$\overline{\int} \overline{f}_{h,L} < \Gamma_0 \cdot \gamma \cdot 2^{-M+1}. \tag{134}$$

We now define the functions $X_{h,L}$ on $\overline{\Lambda}'(q_L)$ for $h = 1, \dots, K$, by setting $X_{h,L}(x) = \overline{X}_{h,L}(x)$ if $x \in \overline{\Lambda}'(q_L)$, $h = 1, \dots, K$; also define

$$f_{h,L} = f'_{h,L-1} \cdot \chi_{\Phi_L} + \overline{f}_{h,L} \text{ for } h = 1, \dots, K. \tag{135}$$

Where $f'_{h,L-1}$ is defined in Section 4.2.4 and Φ_L in Section 4.2.5. It is important that by (89), $\overline{\Xi}(q_L)$, which contains the support of $\overline{f}_{h,L}$ is disjoint from Φ_L which contains the support of $f'_{h,L-1} \cdot \chi_{\Phi_L}$.

Recall from (132) that $\overline{\int} f'_{h,L-1} \leq \overline{\int} f_{h,L-1}$ for $h = 1, \dots, K$.

Using (134) and that $f'_{h,L-1}$ is periodic by τ'_{L-1} and $\Phi_L \subset \mathbb{R} \setminus \overline{\Lambda}'(q_L)$ consists of blocks of length τ'_{L-1}

$$\overline{\int} f_{h,L} \leq \overline{\lambda}(\Phi_L) \cdot \overline{\int} f_{h,L-1} + \Gamma_0 \left(\frac{\gamma}{\overline{\lambda}(\overline{\Lambda}'(q_L))} \right) 2^{-M+1} \overline{\lambda}(\overline{\Lambda}'(q_L)) = (*). \tag{136}$$

Since $\Phi_L \subset \mathbb{R} \setminus \overline{\Lambda}'(q_L)$ by (132) we have

$$\left(\overline{\int} f_{h,L-1} \right) \frac{\overline{\lambda}(\Phi_L)}{\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L))} < \Gamma_0 \cdot C_\gamma 2^{-M+1}.$$

Hence, we can continue our estimation by using (54)

(137)
$$\begin{aligned}(*) &< \left(\overline{\int} f_{h,L-1} \right) \frac{\overline{\lambda}(\Phi_L)}{\overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L))} \cdot \overline{\lambda}(\mathbb{R} \setminus \overline{\Lambda}'(q_L)) + \Gamma_0 C_\gamma 2^{-M+1} \overline{\lambda}(\overline{\Lambda}'(q_L)) \\ &< \Gamma_0 \cdot C_\gamma \cdot 2^{-M+1}.\end{aligned}$$

After these observations we can return to Section 4.2.6, to the definition of $\mathcal{P}_L$ and read everything until the paragraph marked by a †.

When $K > 0$ we need to add the following estimate to the case when $x \in \mathbb{R} \setminus (\overline{\Lambda}'(q_L) \cup E^L) \subset \widetilde{\Phi}_L \subset \Phi_L$.

If $\alpha_L(x) \le n < n+m \le \omega_L(x)$ and $\tau_L(x)|m$ then by (84) and (95) for $h = 1, \dots, K$

(138)
$$\frac{1}{m}\sum_{k=n}^{n+m-1} f'_{h,L-1}(x+k^2) = \frac{1}{m}\sum_{k=n}^{n+m-1} f_{h,L}(x+k^2) > X_{h,L}(x) = X'_{h,L-1}(x).$$

Next suppose $x \in \overline{\Lambda}'(q_L)\setminus E^L \subset \overline{\Lambda}'(q_L)\setminus E_{\delta_L}$. For $h = 1, \dots, K$ the estimates which we have for the $K-M$ family put on $\overline{\Lambda}'(q_L)$ can be applied. In other words, for these x, set $\omega_L(x) \overset{\text{def}}{=} \overline{\omega}_L(x) > \alpha_L(x) \overset{\text{def}}{=} \overline{\alpha}_L(x)$, $\tau_L(x) \overset{\text{def}}{=} \overline{\tau}_L(x) q_L \tau'_{L-1} < \tau_L = q_L \overline{\tau}_L \tau'_{L-1}$. Then $\omega_L^2(x) < \tau_L$, and

$$\frac{\omega_L(x)}{\alpha_L(x)} > \Omega_L \overline{\tau}_L(x) = \Omega \tau_L(x).$$

Furthermore, if $\alpha_L(x) \le n < n+m \le \omega_L(x)$ and $\tau_L(x)|m$, then $\overline{\tau}_L(x)|m$ and by (133) and (135) we have for $h = 1, \dots, K$

$$\frac{1}{m}\sum_{k=n}^{n+m-1} f_{h,L}(x+k^2) > X_{h,L}(x).$$

For all $p \in \mathcal{P}_L \subset \overline{\mathcal{P}}_L$ we have $(\overline{\tau}_L(x) q_L \tau'_{L-1}, p) = (\tau_L(x), p) = 1$ and for $h = 1, \dots, K$, if $\alpha_L^2(x) \le j < j + \tau_L(x) \le \omega_L^2(x)$ then $\alpha_L^2(x) = \overline{\alpha}_L^2(x) \le j < j + \overline{\tau}_L(x) < \dots < j + q_L \tau'_{L-1} \overline{\tau}_L(x) \le \omega_L^2(x) = \overline{\omega}_L^2(x)$ and hence

$$\begin{aligned} f_{h,L}(x+j+\tau_L(x)) = \overline{f}_{h,L}(x+j+\tau_L(x)) &= \overline{f}_{h,L}(x+j+q_L\tau'_{L-1}\overline{\tau}_L(x)) \\ &= \overline{f}_{h,L}(x+j+(q_L\tau'_{L-1}-1)\overline{\tau}_L(x)) \\ &= \dots = \overline{f}_{h,L}(x+j) = f_{h,L}(x+j). \end{aligned}$$

4.2.14. *Case $K > 0$, properties of $f_{K+1,L}$.* This section is again identical to Section 4.2.7.

4.2.15. *Case $K > 0$, finishing the leakage.* We start to argue as in Section 4.2.8. We need to insert just before the sentence containing (119) the remark: Moreover, if $\alpha(x) \le n < n+m \le \omega(x)$ and $\tau(x)|m$, then for all $h = 1, \dots, K$ letting $f_h = f_{h,L''}$ (see also (64) which is used with $L = L''+1$)

$$\frac{1}{m}\sum_{k=n}^{n+m-1} f_h(x+k^2) > X_h(x). \tag{139}$$

Before (120) we need to add the comment that by (136)–(137) for $h = 1, \dots, K$

$$\overline{\int} f_h < C_\gamma \Gamma_0 2^{-M+1} < \Gamma \cdot 2^{-M+1}. \tag{140}$$

The rest of the argument is identical to Section 4.2.8 and this way we can complete our induction. □

5. Proof of the main result

Lemma 5 yields the next theorem which, as we will see, easily implies Theorem 1.

THEOREM 8. *Given* $\delta > 0$, M *and* K *there exist* $\tau_0 \in \mathbb{N}$, $\overline{E}_\delta \subset [0,1)$, *a measurable transformation* $T : [0,1) \to [0,1)$, $T(x) = x + \frac{1}{\tau_0}$ *modulo* 1, $f : [0,1) \to [0,+\infty)$, $\overline{X}_h$, $h = 1, \ldots, K$ *which are pairwise independent* M–0.99-*distributed random variables defined on* $[0,1)$ *equipped with the Lebesgue measure*, λ, *such that* $\lambda(\overline{E}_\delta) < \delta$, *for all* $x \in [0,1) \setminus \overline{E}_\delta$ *there exists* N_x *satisfying*

$$\frac{1}{N_x} \sum_{k=1}^{N_x} f(T^{k^2}(x)) > \sum_{h=1}^{K} \overline{X}_h(x),$$

and $\int_{[0,1)} f d\lambda < K \cdot 2^{-M+2}$.

Proof. Use Lemma 5 with δ, $\Omega = 1000$, $\Gamma = 1.1$, $A = 1$, $\mathcal{P} = \emptyset$ to obtain a $K - M$ family with E_δ, f_h and X_h periodic by $\tau = \tau_0$. Set $\overline{E}_\delta = \frac{1}{\tau_0} E_\delta \cap [0,1)$ and for $x \in [0,1)$ set $\overline{f}_h(x) = 1.01 \cdot f_h(\tau_0 \cdot x)$, $\overline{X}_h(x) = X_h(\tau_0 \cdot x)$.

Assume $x \in [0,1) \setminus \overline{E}_\delta$. Since $\Omega\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x) < \omega(\tau_0 \cdot x)$ we have $\alpha(\tau_0 \cdot x) = n < n + (\Omega - 1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x) < \omega(\tau_0 \cdot x)$ and (37) used with $n = \alpha(\tau_0 \cdot x)$ and $m = (\Omega - 1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x)$ implies

$$\frac{1}{(\Omega-1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x)} \sum_{k=\alpha(\tau_0 \cdot x)}^{\alpha(\tau_0 \cdot x)+(\Omega-1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x)-1} f_h(\tau_0 \cdot (T^{k^2} x))$$

$$= \frac{1}{(\Omega-1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x)} \sum_{k=\alpha(\tau_0 \cdot x)}^{\alpha(\tau_0 \cdot x)+(\Omega-1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x)-1} f_h(\tau_0 \cdot x + k^2) > X_h(\tau_0 \cdot x).$$

Since $f_h \geq 0$, if we let $N_x = \alpha(\tau_0 \cdot x) + (\Omega - 1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x) - 1$, then since $\Omega = 1000$, $N_x/(\Omega - 1)\alpha(\tau_0 \cdot x)\tau(\tau_0 \cdot x) < 1.01$, for all $h = 1, \ldots, K$

$$\frac{1}{N_x} \sum_{k=1}^{N_x} \overline{f}_h(T^{k^2} x) = \frac{1.01}{N_x} \sum_{k=1}^{N_x} f_h(\tau_0 \cdot (T^{k^2} x)) \geq \overline{X}_h(x). \tag{141}$$

Let $f(x)$ be the restriction of $\sum_{h=1}^{K} \overline{f}_h(x)$ onto $[0,1)$. Therefore, using (39) with $\gamma' = 1$ from Lemma 5 we obtain

$$\int_0^1 f(x) d\lambda(x) = 1.01 \sum_{h=1}^{K} \overline{\int} f_h < 1.01 \cdot \Gamma \cdot K \cdot 2^{-M+1} < K \cdot 2^{-M+2}.$$

For all $x \in [0,1) \setminus \overline{E}_\delta$ by (141) there exists N_x such that

$$\frac{1}{N_x} \sum_{k=1}^{N_x} f(T^{k^2} x) > \sum_{h=1}^{K} \overline{X}_h(x). \qquad \square$$

Now we can complete the proof of Theorem 1.

Proof. For each $p \in \mathbb{N}$ set $M_p = 4^p$. On the probability space $([0,1), \lambda)$ consider $M_p - 0.99$-distributed random variables $\overline{X}_h$ for $h = 1, \dots, K$ for a sufficiently large K. Assume that u denotes the mean of these variables. An easy calculation shows that

$$u = \int_{[0,1]} \overline{X}_h(x) d\lambda(x) = \sum_{l=0}^{M_p - 1} 0.99^2 \cdot 2^{-l} \cdot 2^{-M_p + l - 1} > 0.9 \cdot M_p \cdot 2^{-M_p - 1}.$$

By the weak law of large numbers

$$\lambda \left\{ x : \left| \frac{1}{K} \sum_{h=1}^{K} \overline{X}_h(x) - u \right| \geq \frac{u}{2} \right\} \to 0.$$

Fix K so large that

$$\lambda \left\{ x : \frac{1}{K} \sum_{h=1}^{K} \overline{X}_h(x) \geq \frac{u}{2} \right\} > 1 - \frac{1}{p},$$

and let

$$U_p' = \left\{ x : \frac{1}{K} \sum_{h=1}^{K} \overline{X}_h(x) > \frac{0.9}{2} \cdot M_p \cdot 2^{-M_p - 1} \right\}.$$

We have $\lambda(U_p') > 1 - \frac{1}{p}$. By Theorem 8 used with $\delta = \frac{1}{p}$, M_p and K there exist $\tau_0 \in \mathbb{N}$, $\overline{E}_{1/p} \subset [0,1)$ and a periodic transformation $T : [0,1) \to [0,1)$, $T(x) = x + \frac{1}{\tau_0}$ modulo 1, $f : [0,1) \to [0, +\infty)$, $\overline{X}_h$ pairwise independent $M_p - 0.99$-distributed random variables defined on $[0,1)$ such that $\lambda(\overline{E}_{1/p}) < \frac{1}{p}$ and for all $x \in [0,1) \setminus \overline{E}_{1/p}$ there exists N_x such that

$$\frac{1}{N_x} \sum_{k=1}^{N_x} f(T^{k^2} x) > \sum_{h=1}^{K} \overline{X}_h(x)$$

and $\int_{[0,1)} f d\lambda < K \cdot 2^{-M_p + 2}$. Put $U_p = U_p' \setminus \overline{E}_{1/p}$. Then $\lambda(U_p) > 1 - \frac{2}{p}$ and for $x \in U_p$ there exists N_x such that

$$\frac{1}{N_x} \sum_{k=1}^{N_x} f(T^{k^2} x) > \sum_{h=1}^{K} \overline{X}_h(x) > K \cdot \frac{0.9}{2} \cdot M_p \cdot 2^{-M_p - 1}.$$

Thus letting $t_p = K \cdot \frac{0.9}{2} \cdot M_p \cdot 2^{-M_p-1}$, and

$$\widetilde{U}_p = \left\{ x : \sup_N \frac{1}{N} \sum_{k=1}^{N} f(T^{k^2} x) > t_p \right\}$$

we have $U_p \subset \widetilde{U}_p$ and hence $\lambda(\widetilde{U}_p) > 1 - \frac{2}{p}$. On the other hand

$$\frac{\int f d\lambda}{t_p} = \frac{\int |f| d\lambda}{t_p} < \frac{K \cdot 2^{-M_p+2}}{K \cdot \frac{0.9}{2} \cdot M_p \cdot 2^{-M_p-1}} < \frac{32}{M_p}.$$

Hence, $\lambda(\widetilde{U}_p) \to 1$ and $\int |f| d\lambda / t_p \to 0$ as $p \to \infty$. Therefore there is no C for which (2) holds with $\mu = \lambda$. This implies that the sequence $n_k = k^2$ is L^1-universally bad. □

Acknowledgement. The authors thank an anonymous referee for pointing out the use of the Pólya-Vinogradov inequality in Lemma 3. It shortened our original argument. Other comments of the referees also helped to improve the paper.

References

[1] I. ASSANI, Z. BUCZOLICH, and R. D. MAULDIN, Counting and convergence in ergodic theory, *Acta Univ. Carolin. Math. Phys.* **45** (2004), 5–21. MR 2006a:37001 Zbl 1067.37001

[2] ———, An L^1 counting problem in ergodic theory, *J. Anal. Math.* **95** (2005), 221–241. MR 2006c:37002 Zbl 1110.28013

[3] A. BELLOW, Two problems, in *Measure Theory* (Oberwolfach, June 21–27, 1981), *Lecture Notes in Math.* **945**, Springer-Verlag, New York, 1982.

[4] J. BOURGAIN, An approach to pointwise ergodic theorems, in *Geometric Aspects of Functional Analysis* (1986/87), *Lecture Notes in Math.* **1317**, Springer-Verlag, New York, 1988, pp. 204–223. MR 90b:28016 Zbl 0662.47006

[5] ———, On the pointwise ergodic theorem on L^p for arithmetic sets, *Israel J. Math.* **61** (1988), 73–84. MR 89f:28037b Zbl 0642.28011

[6] ———, Almost sure convergence in ergodic theory, in *Almost Everywhere Convergence* (Columbus, OH, 1988), Academic Press, Boston, MA, 1989, pp. 145–151. MR 90k:47017 Zbl 0697.47005

[7] ———, Pointwise ergodic theorems for arithmetic sets, *Inst. Hautes Études Sci. Publ. Math.* (1989), 5–45, with an appendix by the author, Harry Furstenberg, Yitzhak Katznelson and Donald S. Ornstein. MR 90k:28030 Zbl 0705.28008

[8] Z. BUCZOLICH and R. D. MAULDIN, Concepts behind divergent ergodic averages along the squares, in *Ergodic Theory and Related Fields*, vol. 430, A.M.S., Providence, RI, 2007, pp. 41–56. MR 2009c:37001 Zbl 1122.37003

[9] J.-P. CONZE, Convergence des moyennes ergodiques pour des sous-suites, in *Contributions au Calcul des Probabilités*, *Bull. Soc. Math. France*, *Mém.* **35**, Soc. Math. France, Paris, 1973, pp. 7–15. MR 56 #12226 Zbl 0285.28017

[10] H. FURSTENBERG, Problem session, *Conference on Ergodic Theory and Applications,* University of New Hampshire, Durham, NH, June 1982.

[11] G. H. HARDY and E. M. WRIGHT, *An Introduction to the Theory of Numbers*, fifth ed., The Clarendon Press, Oxford Univ. Press, New York, 1979. MR 81i:10002 Zbl 0423.10001

[12] H. IWANIEC and E. KOWALSKI, *Analytic Number Theory*, *A.M.S. Colloq. Publ.* **53**, Amer. Math. Soc., Providence, RI, 2004. MR 2005h:11005 Zbl 1059.11001

[13] P. KURLBERG and Z. RUDNICK, The distribution of spacings between quadratic residues, *Duke Math. J.* **100** (1999), 211–242. MR 2000k:11109 Zbl 0985.11038

[14] I. NIVEN and H. S. ZUCKERMAN, *An Introduction to the Theory of Numbers*, third ed., John Wiley & Sons, New York, 1972. MR 49 #8921 Zbl 0237.10001

[15] R. PERALTA, On the distribution of quadratic residues and nonresidues modulo a prime number, *Math. Comp.* **58** (1992), 433–440. MR 93c:11115 Zbl 0745.11057

[16] J. M. ROSENBLATT and M. WIERDL, Pointwise ergodic theorems via harmonic analysis, in *Ergodic Theory and its Connections with Harmonic Analysis* (Alexandria, 1993), *London Math. Soc. Lecture Note Ser.* **205**, Cambridge Univ. Press, Cambridge, 1995, pp. 3–151. MR 96c:28025 Zbl 0848.28008

[17] S. SAWYER, Maximal inequalities of weak type, *Ann. of Math.* **84** (1966), 157–174. MR 35 #763 Zbl 0186.20503

(Received April 5, 2005)
(Revised May 14, 2008)

E-mail address: buczo@cs.elte.hu
DEPARTMENT OF ANALYSIS, EÖTVÖS LORÁND, UNIVERSITY, PÁZMÁNY PÉTER SÉTÁNY 1/C, 1117 BUDAPEST, HUNGARY
www.cs.elte.hu/∼buczo

E-mail address: mauldin@unt.edu
UNIVERSITY OF NORTH TEXAS, DEPARTMENT OF MATHEMATICS, DENTON 76203-1430, UNITED STATES,

www.math.unt.edu/∼mauldin