Functiones et Approximatio
48.1 (2013), 37–50
doi: 10.7169/facm/2013.48.1.4

ON VAN DER CORPUT PROPERTY OF SHIFTED PRIMES

Siniša Slijepčević

Abstract: We prove that the upper bound for the van der Corput property of the set of shifted primes is $O((\log n)^{-1+o(1)})$, giving an answer to a problem considered by Ruzsa and Montgomery for the set of shifted primes $p-1$. We construct normed non-negative valued cosine polynomials with the spectrum in the set $p-1$, $p \leqslant n$, and a small free coefficient $a_0 = O((\log n)^{-1+o(1)})$. This implies the same bound for the intersective property of the set $p-1$, and also bounds for several properties related to uniform distribution of related sets.

Keywords: Sárközy theorem, recurrence, primes, difference sets, positive definiteness, van der Corput property, Fourier analysis.

1. Introduction

We say that a set of integers $\mathcal{S}$ is a *van der Corput* (or *correlative*) set, if given a real sequence $(x_n)_{n\in N}$, if all the sequences $(x_{n+d} - x_n)_{n\in N}$, $d \in \mathcal{S}$, are uniformly distributed mod 1, then the sequence $(x_n)_{n\in N}$ is itself uniformly distributed mod 1. The property was introduced by Kamae and Mendès France ([2]), and is important as it is closely related to the intersective property of integers, discussed below. Classical examples of van der Corput sets are sets of squares, shifted primes $p+1$, $p-1$, and also sets of values $P(n)$, where P is any polynomial with integer coefficients, and has a solution of $P(n) \equiv 0 \pmod{k}$ for all k. All van der Corput sets are intersective sets, but the converse does not hold, as was shown by Bourgain ([1]).

We first recall the key characterization of the van der Corput property. If $\mathcal{S}$ is a set of positive integers, then let $\mathcal{S}_n = \mathcal{S} \cap \{1, ..., n\}$. We denote by $\mathcal{T}(\mathcal{S})$ the set of all cosine polynomials

$$T(x) = a_0 + \sum_{d\in\mathcal{S}_n} a_d \cos(2\pi dx), \tag{1.1}$$

$T(0) = 1$, $T(x) \geqslant 0$ for all x, where n is any integer and a_0, a_d are real numbers (i.e. T is a non-negative normed cosine polynomial with the spectrum in $\mathcal{S} \cup \{0\}$).

2010 Mathematics Subject Classification: primary: 11P99; secondary: 37A45

Kamae and Mendès France proved that a set is a van der Corput set if and only if ([2], [4])

$$\inf_{T\in\mathcal{T}(\mathcal{S})} a_0 = 0. \tag{1.2}$$

We can define a function which measures how quickly a set is becoming a van der Corput set with

$$\gamma(n) = \inf_{T\in\mathcal{T}(\mathcal{S}_n)} a_0, \tag{1.3}$$

and then a set is van der Corput if and only if $\gamma(n) \to 0$ as $n \to \infty$.

Ruzsa and Montgomery set a problem of finding any upper bound for the function γ for any non-trivial van der Corput set ([4], unsolved problem 3; [7]). Ruzsa in [6] announced the result that for the set of squares, $\gamma(n) = O((\log n)^{-1/2})$, but the proof was never published. The author in [12] proved that for the set of squares, $\gamma(n) = O((\log n)^{-1/3})$. In this paper we prove the following result:

Theorem 1. *If $\mathcal{S}$ is the set of shifted primes $p-1$, then $\gamma(n) = O((\log n)^{-1+o(1)})$.*

The gap between the upper bound and the best available lower bound remains very large, as in the case of the sets of recurrence discussed below. The lower bound below relies on a construction of Ruzsa [8]:

Theorem 2. *If $\mathcal{S}$ is the set of shifted primes $p-1$, then $\gamma(n) \gg n^{\left(-1+\frac{\log 2-\varepsilon}{\log\log n}\right)}$, where $\varepsilon > 0$ is an arbitrary real number.*

Structure of the proof and its limitations. We define a cosine polynomial

$$F_{N,d}(\theta) = \frac{1}{k}\,\mathrm{Re} \sum_{\substack{p\leqslant dN+1\\ p\equiv 1 (\mathrm{mod}\, d)}} \log p\cdot e((p-1)\theta), \tag{1.4}$$

where $e(\theta) = \exp(2\pi i\theta)$ and k is chosen so that $F_{N,d}(0) = 1$. We show in Sections 2 and 3 by using exponential sum estimates along major and minor arcs that

$$F_{N,d}(\theta) \geqslant \tau(d,q) + E(d,q,\kappa,N).$$

Here $\kappa = \theta - a/q$, the function E is the error term and $\tau(d,q)$ is the principal part which is (for square-free d) 1 for $q|d$, 0 if q not square-free, and $-1/\varphi(q/(q,d))$ otherwise (φ being the Euler's totient function and (q,d) the greatest common divisor). In Section 4 we demonstrate that for a given $\delta > 0$, one can find a collection of positive integers $\mathcal{D}$ not exceeding $\exp((\log 1/\delta)^{2+o(1)})$ and weights $\sum_{d\in\mathcal{D}} w(d) = 1$ such that for any integer $q > 0$,

$$\sum_{d\in\mathcal{D}} w(d)\tau(d,q) \geqslant -\delta/2.$$

In addition, one can find constants R, N not exceeding $O(\exp((\log 1/\delta)^{4+o(1)}))$ for any given θ such that if a/q is the Dirichlet's approximation of $\theta = a/q + \kappa$, $\kappa \leqslant 1/(qR)$, then the error term $|E(d,q,\kappa,N)| \leqslant \delta/2$. This seemingly implies effectively the same upper bound for $\gamma(n)$ as obtained in [9] for a stronger intersective property of sets of integers (see below).

Unfortunately, in our calculations the constants R, N can not be chosen so that for all $\theta \in \boldsymbol{T} = \boldsymbol{R}/\boldsymbol{Z}$ the error term is small. Namely, for $d\theta$ close to an integer, the error term is $O(dN/R)$, and for θ on minor arcs, the error term is $O(d^2\sqrt{R}/\sqrt{N})$. We resolve it by choosing a geometric sequence of constants $N_1, \ldots, N_{4/\delta}$, which results with the bound in Theorem 1. We finalize the proof in Section 5 by constructing the required cosine polynomial as a convex combination of $F_{N,d}$ over $d \in \mathcal{D}$ and N_j.

Applications. We say a set $\mathcal{S}$ is *intersective set* (or a *set of recurrence*, or a *Poincaré set)*, if for any set A of integers with positive upper Banach density

$$\rho(A) = \lim \sup_{n\to\infty} |A \cap [1, n]|/n > 0,$$

its difference set $A - A$ contains an element of $\mathcal{S}$. Given any set of integers $\mathcal{S}$, one can define the function $\alpha : \boldsymbol{N} \to [0, 1]$ as $\alpha(n) = \sup \rho(A)$, where A goes over all sets of integers whose difference set does not contain an element of $\mathcal{S} \cap [1, n]$ (equivalent definitions of α can be found in [7]). A set is an intersective set if and only if $\lim_{n\to\infty} \alpha(n) = 0$. Ruzsa in [7] also proved that if $\mathcal{S}$ is a van der Corput set, then it is also an intersective set, and

$$\alpha(n) \leqslant \gamma(n).$$

The bound $\alpha(n) = O((\log n)^{-1+o(1)}) = O(\exp((-1 + o(1)) \log\log n))$ for the set of shifted primes follows then as a corollary of Theorem 1. This is worse than the bound $\alpha(n) = O(\exp(-c\sqrt[4]{\log n}))$ obtained by Ruzsa and Sanders in [9], but better than earlier bounds in [3] and [10].

The function $\gamma(n)$ has different characterizations and further applications discussed in detail in [4]. We discuss in Section 9 the Heilbronn property of the set of shifted primes, which specifies how well the expression $x(p - 1)$ can approximate integers uniformly in $x \in \boldsymbol{R}$, by choosing for a given x some prime $p \leqslant n$ so that $x(p - 1)$ is as close to an integer as possible.

2. The major arcs

If Λ is the von-Mangoldt function, we define as in [9]

$$\Lambda_{N,d}(x) := \begin{cases} \Lambda(dx + 1) & \text{if } 1 \leqslant x \leqslant N \\ 0 & \text{otherwise,} \end{cases}$$

and let $\Lambda_N(x) = \Lambda_{N,1}(x)$. The Fourier transform $\widehat{\cdot} : l^1(\boldsymbol{Z}) \to L^\infty(\boldsymbol{R})$ is defined as the map which takes $f \in l^1(\boldsymbol{Z})$ to $\widehat{f}(\theta) = \sum_{x\in\boldsymbol{Z}} f(x)\overline{e(x\theta)}$, thus $\widehat{\Lambda_{N,d}}(\theta)$ is the exponential sum

$$\widehat{\Lambda_{N,d}}(\theta) = \sum_{x\leqslant N} \Lambda(dx + 1)\overline{e(x\theta)}.$$

The classical estimates for Fourier transforms of $\Lambda_{N,d}(x)$ were optimized by Ruzsa and Sanders to the class of problems studied in this paper. They studied two cases related to the generalized Riemann hypothesis: given a pair of integers $D_1 \geqslant D_0 \geqslant 2$, then there either exists an exceptional Dirichlet character of modulus $d_D \leqslant D_0$ or not ([9], Proposition 4.7). They then obtained the following estimates (we will be more specific below on the assumptions): if $\kappa = \theta - a/q$, where $\theta \in \boldsymbol{T}$, then

$$\left|\widehat{\Lambda_{N,d}}(\theta)\right| \leqslant \frac{|\tau_{a,d,q}|}{\varphi(q)}\widehat{\Lambda_{N,d}}(0) + O\left((1+|\kappa|N)E_{N,D_1}\right), \tag{2.1}$$

$$\left|\widehat{\Lambda_{N,d}}(0)\right| \gg \frac{N}{\varphi(d)} + O\left(E_{N,D_1}\right), \tag{2.2}$$

where

$$E_{N,D_1} = ND_1^2 \exp\left(-\frac{c_1 \log N}{\sqrt{\log N} + \log D_1}\right),$$

$$\tau_{a,d,q} = \sum_{\substack{m=0 \\ (md+1,q)=1}}^{q-1} e\left(m\frac{a}{q}\right).$$

Proposition 1 (Ruzsa, Sanders). *There is an absolute constant c_1 such that for any pair of integers $D_1 \geqslant D_0 \geqslant 2$, one of the following possibilities hold:*

(i) *((D_1, D_0) is exceptional). There is an integer $d_D \leqslant D_0$, such that for all non-negative integers N, a, q, d, where $1 \leqslant dq \leqslant D_1$, $d_D|d$, and $(a,q) = 1$, for any $\theta \in \boldsymbol{T}$ (2.1), (2.2) hold, where $\kappa = \theta - a/q$.*

(ii) *((D_1, D_0) is unexceptional). For all non-negative integers N, a, q, d, where $1 \leqslant dq \leqslant D_0$ and $(a,q) = 1$, for any $\theta \in \boldsymbol{T}$ (2.1), (2.2) hold, where $\kappa = \theta - a/q$.*

Proof. [9], Propositions 5.3. and 5.5. (Note that (2.1) is explicitly obtained at the end of the proof of Proposition 5.3.) ∎

We now define a function τ closely related to $\tau_{a,d,q}$ above, which will be the main term when estimating cosine polynomials $F_{N,d}$. Let

$$\tau(d,q) = \begin{cases} 1, & q|d \\ 0, & (d,r) > 1 \text{ or } r \text{ not square-free} \\ -1/\varphi(r) & \text{otherwise,} \end{cases} \tag{2.3}$$

where $r = q/(q,d)$. Note that for d square-free, the second row condition above is equivalent to q being not square-free.

Lemma 1. *Let a, d, q be positive integers, $(a,q) = 1$, $r = q/(q,d) > 1$ and $a^* = ad/(q,d)$. Then*

$$\frac{|\tau_{a^*,d,r}|}{\varphi(r)} = |\tau(d,q)|. \tag{2.4}$$

Proof. As was noted in [9], Section 5,

$$\tau_{a,d,q} = \begin{cases} c_q(a)e(-m_{d,q}a/q) & \text{if } (d,q)=1 \\ 0 & \text{otherwise,} \end{cases}$$

where $c_q(a)$ is the Ramanujan sum and $m_{d,q}$ is a solution of $m_{d,q}d \equiv 1(\mathrm{mod} q)$. Now if $q|d$, $\tau_{a^*,d,r} = \tau_{a^*,d,1} = 1$, thus both sides of (2.4) are equal to 1. If $(d,r) > 1$, then $\tau_{a^*,d,r} = 0$, and if r not square-free, then $\tau_{a^*,d,r} = 0$ as the Ramanujan sum $c_r(a^*) = 0$ when r not square-free. The remaining case follows from $(a^*, r) = 1$, r square-free implying that the Ramanujan sum $|c_r(a^*)| = 1$. ∎

It is easy to see that there exists a constant c_2 depending only on c_1 such that if

$$\log N \geqslant c_2(\log D_1)^2, \tag{2.5}$$

then

$$D_1^2 \exp\left(-\frac{c_1 \log N}{\sqrt{\log N} + \log D_1}\right) \leqslant \frac{1}{D_1^2}. \tag{2.6}$$

We first discuss the case of q not dividing d, and then $q|d$.

Proposition 2. *Assume all the assumptions of Proposition 1 hold for D_0, D_1, θ, N, a, q, d, κ, and in addition (2.5), (2.6). If q not dividing d, then*

$$F_{N,d}(\theta) \geqslant \tau(d,q) + O\left(\frac{1}{D_1} + |\kappa|N\right).$$

Proof. If we write

$$\psi(x;q,a) = \sum_{\substack{n \leqslant x \\ n \equiv a (\mathrm{mod} q)}} \Lambda(n),$$

$$\vartheta(x;q,a) = \sum_{\substack{p \leqslant x \\ p \equiv a (\mathrm{mod} q)}} \log(p),$$

then $\widehat{\Lambda_{N,d}}(0) = \psi(Nd+1; d, 1)$ and $k = \vartheta(Nd+1; d, 1)$ where k is the denominator in (1.4). By the well-known property of functions ψ, ϑ (see e.g. [5], p.381),

$$\psi(Nd+1; d, 1) - \vartheta(Nd+1; d, 1) \ll \sqrt{dN}.$$

Relations (2.2), (2.6) and $\varphi(d) < D_1$ imply that

$$\frac{N}{\left|\widehat{\Lambda_{N,d}}(0)\right|} \ll D_1. \tag{2.7}$$

If we use the shorthand notation $F = \mathrm{Re} \sum_{p \leqslant dN+1, p \equiv 1 (\mathrm{mod} d)} \log p \cdot e((p-1)\theta)$, and then $F_{N,d}(\theta) = F/k$, we see from definitions that F is approximately $\mathrm{Re}\, \widehat{\Lambda_{N,d}}(d\theta)$, or more precisely

$$|\mathrm{Re}\, \widehat{\Lambda_{N,d}}(d\theta) - F| \leqslant \widehat{\Lambda_{N,d}}(0) - k \ll \sqrt{dN}.$$

Putting these three inequalities together,

$$\left|\frac{F}{k} - \frac{\operatorname{Re}\widehat{\Lambda_{N,d}}(d\theta)}{\widehat{\Lambda_{N,d}}(0)}\right| \leqslant \left|\frac{F}{k}\right| \frac{|\widehat{\Lambda_{N,d}}(0) - k|}{|\widehat{\Lambda_{N,d}}(0)|} + \frac{|\operatorname{Re}\widehat{\Lambda_{N,d}}(d\theta) - F|}{|\widehat{\Lambda_{N,d}}(0)|} \ll \frac{\sqrt{d}}{\sqrt{N}} D_1. \quad (2.8)$$

Now if $\theta - a/q = \kappa$, then $d\theta - a^*/r = d\kappa$, where $a^* = ad/(d,q)$, $r = q/(d,q)$. Combining (2.1), (2.2), (2.6) and (2.7) we easily get that

$$\left|\frac{\widehat{\Lambda_{N,d}}(d\theta)}{\widehat{\Lambda_{N,d}}(0)}\right| \leqslant \frac{|\tau_{a^*,d,r}|}{\varphi(r)} + O\left(\frac{1}{D_1} + |\kappa|N\right).$$

The last two relations combined (noting that if $d \leqslant D_1$ and (2.5), then $\sqrt{d}D_1/\sqrt{N} \ll 1/D_1$) and Lemma 1 complete the proof. ∎

Proposition 3. *Say d, N are positive integers, $\theta \in \boldsymbol{T}$, and $\kappa = \theta - a/q$, $(a,q) = 1$ and $q|d$. Then*

$$F_{N,d}(\theta) \geqslant 1 + O(dN|\kappa|). \quad (2.9)$$

Proof. We first recall that $\operatorname{Re} e(\theta) = \cos(2\pi\theta) \geqslant 1 - 2\pi\,\|\theta\|$, where $\|.\|$ is the distance from the nearest integer. Thus if $|dN\kappa| \leqslant 1/2$, then for each $p \leqslant dN + 1$, $d|(p-1)$, we get $\|(p-1)\theta\| = (p-1)|\kappa|$ and $\operatorname{Re} e((p-1)\theta) \geqslant 1 - 2\pi dN|\kappa|$, which easily implies (2.9). ∎

3. The minor arcs

We start with the minor arc estimate from [9], Corollary 6.2, which is derived from the classical result of Vinogradov ([4], Theorem 2.9).

Proposition 4. *Suppose that $d \leqslant N$ and $q \leqslant R$ are positive integers, $\theta \in \boldsymbol{T}$, $(a,q) = 1$ and $|\theta - a/q| \leqslant 1/qR$. Then*

$$\left|\widehat{\Lambda_{N,d}}(\theta)\right| \ll d(\log N)^4 \left(\frac{N}{\sqrt{q}} + N^{4/5} + \sqrt{NR}\right). \quad (3.1)$$

The minor arc estimate for $F_{N,d}(\theta)$ now follows.

Corollary 1. *Suppose $d \leqslant D_1$, $q \leqslant R$, N are positive integers, $\theta \in \boldsymbol{T}$, $(a,q) = 1$ and $|\theta - a/q| \leqslant 1/qR$. Assume also (2.5) and (2.6) hold. Then*

$$|F_{d,N}(\theta)| \ll D_1^2(\log N)^4 \left(\frac{1}{\sqrt{q}} + N^{-1/5} + \frac{\sqrt{R}}{\sqrt{N}}\right). \quad (3.2)$$

Proof. First note that as $d \leqslant D_1$, Proposition 1 implies that (2.2) holds. Then similarly as in the proof of Proposition 2,

$$\frac{N}{\left|\widehat{\Lambda_{N,d}}(0)\right|} \ll D_1 \quad (3.3)$$

and

$$\left|\frac{F}{k}-\frac{\mathrm{Re}\widehat{\Lambda_{N,d}}(d\theta)}{\widehat{\Lambda_{N,d}}(0)}\right| \ll \frac{\sqrt{d}}{\sqrt{N}}D_1 \leqslant \frac{D_1^{3/2}}{\sqrt{N}}. \tag{3.4}$$

We complete the proof by combining (3.1), (3.3) and (3.4). ■

4. Cancelling out the main term

Recall the definition of the arithmetic function τ in (2.3). We first cancel out the main terms in the unexceptional case.

Theorem 3. *For a given $\delta > 0$ smaller than some $\delta_0 > 0$ there exists a collection of positive integers $\mathcal{D}$ not greater than $\exp((\log 1/\delta)^{2+o(1)})$ and weights $w : \mathcal{D} \to \boldsymbol{R}$, $\sum_{d\in\mathcal{D}} w(d) = 1$, such that for all positive integers q,*

$$\sum_{d\in\mathcal{D}} w(d)\tau(d,q) \geqslant -\delta/2. \tag{4.1}$$

Proof. We first define the set $\mathcal{D}$ depending on three constants $p^- < p^+$, l to be defined below. Let

$$d^* = \prod_{p\leqslant p^-} p$$

(p denoting a product over primes as usual), and let $\mathcal{D}(j)$ be the set of all square-free numbers d^*d, d containing in its decomposition only primes $p^- < p \leqslant p^+$, and such that $\omega(d) = j$, where $\omega(d)$ denotes the number of distinct primes dividing d. We set now

$$\begin{aligned}
p^+ &= 2/\delta + 1,\\
l &= \left\lceil 2\log(1/\delta)\left(\frac{2\log\log(2/\delta)}{\log 2}+1\right)\right\rceil = \log(1/\delta)^{1+o(1)},\\
p^- &= 2l^2 + 1 = \log(1/\delta)^{2+o(1)},\\
\mathcal{D} &= \mathcal{D}(l),\\
W(j) &= \sum_{d^*d\in\mathcal{D}(j)} 1/\varphi(d),\\
w(d^*d) &= \frac{1}{W(l)}\frac{1}{\varphi(d)},
\end{aligned}$$

where $\lceil x\rceil$ is the smallest integer $\geqslant x$. We denote the left-hand side of (4.1) with $A(q)$.

By using $\prod_{p\leqslant x} p = \exp(x^{(1+o(1))})$ (see e.g. [5], Corollary 2.6), we easily see that for each $d^*d \in \mathcal{D}$,

$$d^*d \leqslant \prod_{p\leqslant p^-} p\cdot(p^+)^l = \exp(\log(1/\delta)^{2+o(1)}).$$

If q is not square-free or q contains a prime larger than p^+, the claim $A(q) \geqslant -\delta/2$ is straightforward as for all d, $\tau(d,q) = 0$, respectively $\tau(d,q) \geqslant -1/\varphi(p^+) \geqslant -\delta/2$.

We can now without loss of generality assume that q is square-free, containing no prime $> p^+$ or $\leqslant p^-$ in its decomposition (the latter can be eliminated as primes $\leqslant p^-$ do not affect the value of $\tau(d^*d, q)$ for square-free q). We define the following constants and sets to assist us in calculations:

$$\begin{aligned} k &= \log(1/\delta), \\ \mathcal{D}(j;q) &= \{d^*d \in \mathcal{D}(j),\ (d,q) = 1\}, \\ W(j;q) &= \sum_{d^*d \in \mathcal{D}(j,q)} 1/\varphi(d), \\ W = W(1) &= \sum_{p^- < p \leqslant p^+} \frac{1}{\varphi(p)} = \sum_{p^- < p \leqslant p^+} \frac{1}{p-1}. \end{aligned}$$

The remaining cases will be distinguished by $\omega(q)$.

(i) Assume $\omega(q) \leqslant 2k$. We will show that the terms for which $q|d$ dominate all the others. We first show the following: for $j_1 < j_2$,

$$W(j_2;q) \leqslant \frac{W^{j_2-j_1} W(j_1;q)}{j_2(j_2-1)...(j_1+1)}. \tag{4.2}$$

Indeed, if we define

$$W^*(j;q) = \sum_{(p_1,p_2,\ldots,p_j)} \frac{1}{\varphi(p_1 p_2 \ldots p_j)},$$

where the sum goes over all ordered j-tuples of pairwise different primes p_i, $p^- < p_i \leqslant p^+$, p_i coprime with q, then $W(j;q) = W^*(j;q)/j!$. However, as φ is multiplicative for coprime integers,

$$W^*(j_2;q) \leqslant W^{j_2-j_1} W^*(j_1;q) \tag{4.3}$$

(we first choose the first $j_2 - j_1$ primes and then the remaining j_1). We obtain (4.2) by dividing (4.3) with $j_2!$.

The definition of $A(q)$ now yields:

$$A(q) = \sum_{q|d} \frac{1}{\varphi(d)} - \sum_{q/(q,d)>1} \frac{1}{\varphi(d)} \frac{1}{\varphi(r)},$$

where the sums above and below are over $d^*d \in \mathcal{D}$ unless specified otherwise and r always denotes $r = q/(q,d)$ (recall that we assumed that q and d^* are coprime). We first detail out the first term:

$$\sum_{q|d} \frac{1}{\varphi(d)} = \sum_{d^*d \in \mathcal{D}(l-\omega(q);q)} \frac{1}{\varphi(d)} \frac{1}{\varphi(q)} = W(l-\omega(q);q) \frac{1}{\varphi(q)}.$$

If $\omega((d,q))=j$, we can choose (d,q) as a factor of q in $\binom{\omega(q)}{j}$ ways. Using that, (4.2) and in the last rows $\omega(q)\leqslant 2k$ and $(1+x/n)^n<\exp(x)$ we obtain

$$\begin{aligned}\sum_{q/(q,d)>1}\frac{1}{\varphi(d)}\frac{1}{\varphi(r)} &= \sum_{j=0}^{\omega(q)-1}\sum_{\omega((d,q))=j}\frac{1}{\varphi(d)}\frac{1}{\varphi(r)} = \sum_{j=0}^{\omega(q)-1}W(l-j;q)\binom{\omega(q)}{j}\frac{1}{\varphi(q)}\\ &\leqslant \sum_{j=0}^{\omega(q)-1}\frac{W^{\omega(q)-j}}{(l-j)...(l-\omega(q)+1)}\binom{\omega(q)}{j}\cdot\frac{W(l-\omega(q);q)}{\varphi(q)}\\ &\leqslant \frac{W(l-\omega(q);q)}{\varphi(q)}\sum_{j=0}^{\omega(q)-1}\binom{\omega(q)}{j}\frac{W^{\omega(q)-j}}{(l-\omega(q))^{\omega(q)-j}}\\ &\leqslant \frac{W(l-\omega(q);q)}{\varphi(q)}\left[\left(1+\frac{W}{(l-2k)}\right)^{2k}-1\right]\\ &< \frac{W(l-\omega(q);q)}{\varphi(q)}\left[\exp\left(\frac{W}{l/(2k)-1}\right)-1\right].\end{aligned}$$

As by e.g. [5], Theorem 2.7.(d),

$$\sum_{p\leqslant x}\frac{1}{p-1}=\log\log x\cdot(1+o(1)), \tag{4.4}$$

we get that

$$W=\sum_{p^-<p\leqslant p^+}\frac{1}{p-1}=\log\log(p^+)(1+o(1))\leqslant 2\log\log(2/\delta). \tag{4.5}$$

It is easy to check that the definitions of l,k imply that

$$1-\left[\exp\left(\frac{2\log\log(2/\delta)}{l/(2k)-1}\right)-1\right]\geqslant 0.$$

Putting all of the above together we get $A(q)>0$.

(ii) Assume $2k<\omega(q)\leqslant 2l$. We now show that all the terms are small. First assume $\omega((q,d))=j\geqslant k$. By the same reasoning as in (4.2) one gets for $j\leqslant l$,

$$W(l;q)=\frac{(W-\sum_{p|q}1/\varphi(p))^{l-j}W(j;q)}{l(l-1)...(j+1)}.$$

Now by definition, $W(l)\geqslant W(l;q)$. Applying again (4.4) we see that for δ small enough,

$$W-\sum_{p|q}1/\varphi(p)\geqslant\log\log(p^+)(1+o(1))-\log\log(2l)(1+o(1))\geqslant 1.$$

Combining all of it one gets

$$\frac{W(j;q)}{W(l)} \leqslant l^{l-j}.$$

Furthermore, as by the Stirling's formula $k! \geqslant k^k \exp(-k)$ and as $k = \log(1/\delta)$, we get for δ small enough

$$\frac{l}{k!} \leqslant \frac{\log(1/\delta)^{(1+o(1))}}{\log(1/\delta)^{\log(1/\delta)}\exp(-(\log(1/\delta))} \leqslant \delta/4.$$

Putting it all that together and summing over $d^*d \in \mathcal{D}$ similarly as above we get

$$\begin{aligned}
\sum_{j=k}^{l}\sum_{\omega((d,q))=j} |w(d^*d)\tau(d^*d,q)| &= \frac{1}{W(l)}\sum_{j=k}^{\min\{l,\omega(q)\}}\sum_{\omega(d,q)=j}\frac{1}{\varphi(d)}\frac{1}{\varphi(r)}\\
&= \sum_{j=k}^{\min\{l,\omega(q)\}}\binom{\omega(q)}{j}\frac{W(l-j;q)}{W(l)}\frac{1}{\varphi(q)}\\
&\leqslant \sum_{j=k}^{\min\{l,\omega(q)\}}\frac{(2l)^j}{j!}l^j\frac{1}{(p^- - 1)^{\omega(q)}}\\
&\leqslant \frac{1}{k!}\sum_{j=k}^{\min\{l,\omega(q)\}}\left(\frac{2l^2}{p^- - 1}\right)^{\omega(q)} \leqslant \frac{l}{k!} \leqslant \delta/4. \qquad (4.6)
\end{aligned}$$

For $\omega((q,d)) = j < k$, $\omega(r) = \omega(q) - j > k$ (where $r = q/(q,d)$). We now see that for $\delta > 0$ small enough,

$$|\tau(d^*d,q)| = 1/\varphi(r) \leqslant 1/(p^- - 1)^k = \log(1/\delta)^{(-2-o(1))\log(1/\delta)} \leqslant \delta/4, \qquad (4.7)$$

thus

$$\sum_{j=0}^{k-1}\sum_{\omega((d,q))=j}|w(d^*d)\tau(d^*d,q)| \leqslant \frac{\delta}{4}\sum_{d^*d\in\mathcal{D}}|w(d^*d)| = \delta/4. \qquad (4.8)$$

Relations (4.6) and (4.8) give $|A(q)| \leqslant \delta/2$.

(iii) Assume $2l < \omega(q)$. Then it is enough to see that for all $d^*d \in \mathcal{D}$, $\omega(r) \geqslant l > k$. We now obtain in the same way as in (4.7) that $|\tau(d^*d,q)| \leqslant \delta/4$, but now for all $d^*d \in \mathcal{D}$, thus $|A(q)| \leqslant \delta/4$. ■

We now modify this for the exceptional case.

Theorem 4. *Assume $\delta > 0$ is smaller than some $\delta_0 > 0$ and let d_D be a positive integer, $d_D = \exp((\log 1/\delta)^{2+o(1)})$. Then there exists a collection of positive integers $\mathcal{D}$, such that $d_D | d$ for all $d \in \mathcal{D}$, not greater than $\exp((\log 1/\delta)^{2+o(1)})$ and weights $w : \mathcal{D} \to \boldsymbol{R}$, $\sum_{d\in\mathcal{D}} w(d) = 1$, such that for all positive integers q,*

$$\sum_{d\in\mathcal{D}} w(d)\tau(d,q) \geqslant -\delta/2. \qquad (4.9)$$

Proof. We define $d^* = d_D \prod_{p \leqslant p^-} p$, where p^- and all the other constants remain the same as in the proof of Theorem 3. Let $\mathcal{D}$ be the set of all the numbers $d^* d$, d square-free, relatively prime with d^*, containing in its decomposition only primes $p^- < p \leqslant p^+$, and such that $\omega(d) = l$. The rest of the proof is analogous as the proof of Theorem 3 with all calculations the same, thus omitted. ∎

5. Proof of Theorem

We complete the proof of Theorem 1 in this section. We will choose below the constants Q, R, and will use the major arcs estimates for $q \leqslant Q$ and minor arcs estimates for $Q < q \leqslant R$. We will assume that a/q is the Dirichlet's approximation of $\theta \in \boldsymbol{T}$, $|\theta - a/q| \leqslant 1/qR$, $(a, q) = 1$. The error terms in Propositions 2, 3 are then

$$E_1 = O\left(\frac{1}{D_1} + \frac{N}{R}\right),$$
$$E_2 = O\left(D_1 N/R\right),$$

as $|\kappa| = 1/qR$ and $d \leqslant D_1$. The error term for minor arcs is the entire right-hand side of (3.2), thus as $q > Q$, it is

$$E_3 = O\left(D_1^2 (\log N)^4 \left(\frac{1}{\sqrt{Q}} + N^{-1/5} + \frac{\sqrt{R}}{\sqrt{N}}\right)\right).$$

To complete the proof, we need to choose the constants D_1, N, Q, R so that the error terms $E_1, E_2, E_3 \leqslant \delta/2$ for all $\theta \in \boldsymbol{T}$ on major; respectively minor arcs. As was noted in the introduction, this is impossible, so we proceed as follows. We define

$$Q = \exp(\log(1/\delta)^{2+o(1)})$$

(the constant obtained as the upper bound on $\mathcal{D}$ in Theorem 3), and let

$$D_0 = Q^2, \qquad D_1 = Q^4.$$

If (D_0, D_1) is unexceptional, we construct the set $\mathcal{D}$ according to Theorem 3, and if it is exceptional with the modulus of the exceptional character $d_D \leqslant D_0$, then according to Theorem 4. Now let $N_0 = \exp(c_2 (\log D_1)^2)$, where c_2 is the constant in (2.5). We now define

$$N_j = N_0 D_1^{8j},$$
$$R_j^* = N_0 D_1^{8k+2},$$

where $j = 1, ..., m$, $4/\delta \leqslant m < 4/\delta + 1$. Then for $0 < \delta \leqslant \delta_0$ for some δ_0 small enough, and $j \leqslant j^*$, it is easy to see that the error terms $E_1, E_2 \leqslant \delta/4$ for the constants $Q, D_1, N_j, R_{j^*}^*$. Furthermore, if $j \geqslant j^* + 1$, the error term $E_3 \leqslant \delta/4$ for the constants $Q, D_1, N_j, R_{j^*}^*$.

Let for a given $\theta \in \boldsymbol{T}$ the rational a_j^*/q_j^*, (a_j^*, q_j^*) be the Dirichlet's approximation of θ, $|\theta - a_j^*/q_j^*| \leqslant 1/q_j^* R_j^*$. Without loss of generality, we can also assume that a_j^*/q_j^* is the rational with the smallest q_j^* for a given R_j^*. Then the sequence q_j^* is increasing.

Let j_0 be the smallest index such that $q_{j_0}^* > Q$ ($q_{j_0}^* = m+1$ if $q_j^* \leqslant Q$ for all j). We define

$$\begin{aligned} a_j/q_j &= a_{j_0-1}^*/q_{j_0-1}^*, &\qquad R_j &= R_{j_0-1}^* \quad \text{for } \ j \leqslant j_0 - 1, \\ a_j/q_j &= a_{j_0}^*/q_{j_0}^*, &\qquad R_j &= R_{j_0}^* \quad \text{for } \ j \geqslant j_0. \end{aligned}$$

Now one can easily check that for any $d \in \mathcal{D}$ and any $j \leqslant j_0 - 1$, the assumptions of Proposition 2 in the case q not dividing d, respectively of Proposition 3 in the case $q|d$, do hold for the constants $D_0, D_1, Q, a_j, q_j, R_j, N_j$, and as was noted above, $E_1, E_2 \leqslant \delta/4$, thus

$$F_{d,N_j}(\theta) \geqslant \tau(d, q_j) - \delta/4. \tag{5.1}$$

Similarly for $j \geqslant j_0 + 1$ and $d \leqslant D_1$, the assumptions of Corollary 1 hold and $E_3 \leqslant \delta/4$, therefore

$$F_{d,N_j}(\theta) \geqslant -\delta/4. \tag{5.2}$$

Also by definition,

$$F_{d,N_{j_0}}(\theta) \geqslant -1. \tag{5.3}$$

Now the required polynomial is

$$T = \frac{1}{m} \sum_{d \in \mathcal{D}} \sum_{j=1}^{m} w(d) F_{d,N_j}.$$

By applying (5.1), (5.2), (5.3) for $1/m$ the sum over j, and (4.1) respectively (4.9) for the sum over $d \in \mathcal{D}$, we get that for any $\theta \in \boldsymbol{T}$, $T(\theta) \geqslant -\delta$. As the largest non-zero coefficient in T is $dN_m \leqslant N_0 D_1^{8(4/\delta+1)+1} = \exp((1/\delta)^{1+o(1)})$, this completes the proof.

6. The lower bound

In this section we prove Theorem 2 on the lower bound for $\gamma(n)$ associated to the set $p-1$. Ruzsa in [8], Section 5, constructed for a given n a subset A of integers not larger than n, $|A| \gg n^{((\log 2 - \varepsilon)/\log\log n)}$ such that $A - A$ contains no shifted prime $p-1$. We now construct a set B of positive integers by the following rule: if $x \equiv a (\mathrm{mod} 2n)$, then $x \in B$ for $a \in A$, otherwise $x \notin B$. Now clearly the upper Banach density of B satisfies

$$\rho(B) \gg n^{(-1+(\log 2-\varepsilon)/\log\log n)} \tag{6.1}$$

and B contains no shifted prime $p-1$ smaller than n. Recall the measure of intersectivity $\alpha(n)$ defined in the introduction, satisfying $\gamma \geqslant \alpha$. As $\alpha(n)$ is by definition $\gg$ than the right-hand side of (6.1), the proof is completed.

7. Application: Heilbronn property of shifted primes

An estimate for the Heilbronn property of shifted primes is an example of an application of Theorem 1. If $\mathcal{H}$ is a set of positive integers, we say that it is a Heilbronn set if $\eta = 0$, where

$$\eta = \sup_{\theta \in \boldsymbol{T}} \inf_{h \in \mathcal{H}} ||h\theta||$$

(for more detailed discussion, see [4], Section 2.7 or [11]). One can quantify the Heilbronn property similarly as the van der Corput and Poincaré properties of integers, and define

$$\eta(n) = \sup_{\theta \in \boldsymbol{T}} \inf_{h \in \mathcal{H}_n} ||h\theta||, \tag{7.1}$$

where $\mathcal{H}_n = \mathcal{H} \cap \{1, ..., n\}$. One can show that a set is a Heilbronn set if and only if $\lim_{n\to\infty} \eta(n) = 0$ ([4], Section 2.7). All van der Corput sets are Heilbronn sets (the converse does not hold), and as was shown in [4], Theorem 2.9,

$$\eta(n) \leqslant \gamma(n). \tag{7.2}$$

Various estimates for the function η have been obtained by Schmidt [11] for sets of values of polynomials with integer coefficients. An upper bound for the set of shifted primes follows from Theorem 1 and (7.2).

Corollary 2. *If η is the arithmetic function (7.1) associated to the set of shifted primes $\mathcal{H}$, then $\eta(n) = O((\log n)^{-1+o(1)})$.*

Acknowledgement. The author thanks the anonymous referee for suggesting an improvement of an early version of the paper which substantially improved the upper bound in the main result.

References

[1] J. Bourgain, *Ruzsa's problem on sets of recurrence*, Israel J. Math. **59** (1987), 151–166.

[2] T. Kamae and M. Mendès France, *Van der Corput's difference theorem*, Israel J. Math. **31** (1977), 335–342.

[3] J. Lucier, *Difference sets and shifted primes*, Acta Math. Hungar. **120** (2008), 79–102.

[4] H.L. Montgomery, *Ten lectures on the Interface Between Analytic Number Theory and Harmonic Analysis,* AMS (1994), CMBS Regional Conference Series in Mathematics, 84.

[5] H.L. Montgomery and R.C. Vaughan, *Multiplicative Number Theory, I. Classical Theory*, Cambridge University Press (2007).

[6] I.Z. Ruzsa, *Uniform distribution, positive trigonometric polynomials and difference sets*, in Semin. on Number Theory. Univ. Bordeaux I, 1981-82. No. 18.

[7] I.Z. Ruzsa, *Connections between the uniform distribution of a sequence and its differences*, Topics in Classical Number Theory, Vol. I, II (Budapest, 1981), 1419–1443, Colloq. Math. Soc. Jànos Bolyai, **34**, North-Holland, Amsterdam (1984).
[8] I.Z. Ruzsa, *On measures of intersectivity*, Acta Math. Hungar. **43** (1984), 335–340.
[9] I.Z. Ruzsa and T. Sanders, *Difference sets and the primes*, Acta Arith. **131** (2008), 281–301.
[10] A. Sárközy, *On difference sets of integers III*, Acta Math. Acad. Sci. Hungar. **31** (1978), 355–386.
[11] W.M. Schmidt, *Small fractional parts of polynomials*, Regional Conference Series No. 32, Amer. Mat. Soc., Providence (1977).
[12] S. Slijepčević, *On van der Corput property of squares*, Glas. Mat. Ser. III (2010), no. 2, 357–372.

Address: Siniša Slijepčević: Department of Mathematics, Bijenička 30, Zagreb, Croatia.

E-mail: slijepce@math.hr

Received: 27 September 2010; **revised:** 4 November 2011