INCOMPLETE EXPONENTIAL SUMS AND DIFFIE–HELLMAN TRIPLES

BY WILLIAM D. BANKS

Department of Mathematics, University of Missouri

Columbia, MO 65211, *USA*

e-mail: `bbanks@math.missouri.edu`

JOHN B. FRIEDLANDER

Department of Mathematics, University of Toronto

Toronto, Ontario M5S 3G3, Canada

e-mail: `frdlndr@math.toronto.edu`

SERGEI V. KONYAGIN

Department of Mechanics and Mathematics, Moscow State University

Moscow, 119992, *Russia*

e-mail: `konyagin@ok.ru`

AND

IGOR E. SHPARLINSKI

Department of Computing, Macquarie University

Sydney, NSW 2109, *Australia*

e-mail: `igor@ics.mq.edu.au`

(*Received November* 2003)

Abstract

Let p be a prime and ϑ an integer of order t in the multiplicative group modulo p. In this paper, we continue the study of the distribution of *Diffie–Hellman triples* $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ by considering the closely related problem of estimating exponential sums formed from linear combinations of the entries in such triples. We show that the techniques developed earlier for complete sums can be combined, modified, and developed further to treat incomplete sums as well. Our bounds imply uniformity of distribution results for Diffie–Hellman triples as the pair (x, y) varies over small boxes.

1. *Introduction*

Let p be a prime and ϑ an integer of order $t \mid p-1$ in the multiplicative group modulo p, that is, $\vartheta^t \equiv 1 \pmod p$ but $\vartheta^j \not\equiv 1 \pmod p$ for $1 \le j < t$. In this paper we continue the study of the distribution of *Diffie–Hellman triples* $(\vartheta^x, \vartheta^y, \vartheta^{xy})$ as initiated in [**5**]; see also [**4**, **8**, **10**]. Here we are interested in the case when the exponents x and y belong to an aligned box inside the square $[1, t]^2$, thus we are led to the problem of estimating exponential sums with a linear combination of the entries $\vartheta^x, \vartheta^y, \vartheta^{xy}$ in such triples.

For integers a, b, c and subsets $\mathcal{X}, \mathcal{Y}$ of $\{1, \ldots, t\}$ we consider the double exponential sum defined by

$$S_{a,b,c}(\mathcal{X}, \mathcal{Y}) = \sum_{x \in \mathcal{X},\ y \in \mathcal{Y}} \mathbf{e}_p\left(a\vartheta^x + b\vartheta^y + c\vartheta^{xy}\right),$$

where as usual $\mathbf{e}_q(z) = \exp(2\pi i z/q)$ for all $q \in \mathbb{N}$ and $z \in \mathbb{R}$.

When ϑ is a primitive root modulo p (that is, when $t = p-1$) and $\mathcal{X}$ and $\mathcal{Y}$ are intervals, such double exponential sums have been introduced and estimated in [**5**]. For complete sums (that is, when $\mathcal{X} = \mathcal{Y} = \{1, \ldots, t\}$), the results of [**5**] have been improved (and extended to arbitrary $t \,|\, p-1$) in [**4**].

In this paper we show that the techniques of [**4**] and [**5**] can be combined and applied to incomplete sums. As in [**4**, **5**], we focus on estimates for sums of the form

$$V_{a,c}(\mathcal{X}, \mathcal{Y}) = \sum_{y \in \mathcal{Y}} \left| \sum_{x \in \mathcal{X}} \mathbf{e}_p \left(a\vartheta^x + c\vartheta^{xy} \right) \right|^4 ,$$

for which the Hölder inequality implies

$$|S_{a,b,c}(\mathcal{X}, \mathcal{Y})|^4 \le (\#\mathcal{Y})^3 \, V_{a,c}(\mathcal{X}, \mathcal{Y}).$$

Throughout we take $\mathcal{X} = \{L+1, \ldots, L+H\}$, $\mathcal{Y} = \{M+1, \ldots, M+K\}$. Due to periodicity, there is no loss of generality if we assume $1 \le H \le t$, $1 \le K \le t$ and hence we do so. This restriction will be convenient in a number of places in the proofs.

The sums $S_{a,b,c}(\mathcal{X}, \mathcal{Y})$ and $V_{a,c}(\mathcal{X}, \mathcal{Y})$ arise naturally in number theory and we expect that the bounds presented here will find applications similar to those derived from bounds for single exponential sums with exponential functions, the theory of which is rather well developed; see [**12**, **13**, **14**, **15**, **16**].

The study of double exponential sums of exponential type has also been motivated by several applications to cryptography, for example to show the uniform distribution of the Diffie–Hellman triples; see [**5**] for details, and also [**2**, **4**]. More precise information about the distribution of these triples over incomplete blocks follows from the results given herein. Various other applications and generalisations of the results of [**4**, **5**] can be found in [**1**, **7**, **8**, **9**, **10**, **11**, **18**].

There is a standard method (see the final section of the paper) whereby incomplete exponential sums of various types may be successfully bounded once bounds are given for the corresponding complete sums. Such a method can be quickly applied in our case, and it leads to a bound which is fairly good when the range for x and y is almost complete. In the more interesting case when the sums are shorter we are able to improve on this result by combining elements in the proofs of [**4**] and [**5**] and adding new ingredients, rather than directly applying the statement for the complete sum. In particular, we obtain a new upper bound on the number of solutions of n-term exponential equations which we hope may find several other applications.

Throughout the paper, the implied constants in the symbols 'O' and '$\ll$' are absolute unless specified otherwise. We also adopt the convention that $[a, b]$ denotes the set of *integers* x with $a \le x \le b$; for instance, below we write $\mathcal{X} = [L+1, L+H]$ instead of $\mathcal{X} = \{L+1, \ldots, L+H\}$.

Acknowledgements. We wish to thank Jean Bourgain for making available to us his preprint [**3**] (see the final section), and Andrei Borodin for calling our attention to an error in the earlier version of the manuscript. During the preparation of this paper, W. B. was supported in part by NSF grant DMS-0070628, J. F. was supported in part by NSERC grant A5123 and by a Killam Research Fellowship, S. K. was supported in part by grants 02-01-00248 from the Russian Foundation for Basic Research and by NSh-3004.2003.1, and I. S. was supported in part by ARC grant DP0211459.

2. *Preparations*

In this section we follow to some extent the ideas in Section 3 of [**4**] and Section 3 of [**5**]. However, we consider the more general case of incomplete sums as opposed to summing over the full period t, and for this some new ideas lead to stronger results.

First, we recall the following well-known identity:

Lemma 1. *For any integer u, one has*

$$\sum_{\lambda=0}^{p-1} \mathbf{e}_p(\lambda u) = \begin{cases} 0 & \text{if } u \not\equiv 0 \pmod p, \\ p & \text{if } u \equiv 0 \pmod p. \end{cases}$$

Proof. See, for example, Exercise 11.a in Chapter 3 of [**19**]. □

For integers a, b, k, L, H with $1 \le H \le t$ we define the exponential sum

$$\sigma_k(a, b; L, H) = \sum_{x=L+1}^{L+H} \mathbf{e}_p\left(a\vartheta^{kx}\right) \mathbf{e}_t(bx).$$

We need the following upper bound on the size of such sums:

Lemma 2. *With the notation as above, suppose that* $\gcd(a, p) = 1$ *and that* $\gcd(k, t) = \delta$*. Then for any integers b, L, H with $1 \le H \le t/\delta$, the following bound holds:*

$$\sigma_k(a, b; L, H) \ll p^{1/2} \log p.$$

Proof. For the case $b = 0$, this statement is equivalent to Lemma 2 of [**13**] or Theorem 8.2 of [**16**]; the general case can be obtained using the same techniques without any further adjustments. □

From Lemma 2 we immediately derive the bound

$$\sigma_k(a, b; L, H) \ll \left(\frac{\delta H}{t} + 1\right) p^{1/2} \log p \qquad (2{\cdot}1)$$

for any $H \ge 1$ provided that $\gcd(a, p) = 1$.

Lemma 3. *For integers b, L, H with $1 \le H \le t$ the following identity holds:*

$$\sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, b; L, H)|^2 = Hp.$$

Proof. Indeed,

$$\begin{aligned}\sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, b; L, H)|^2 &= \sum_{\lambda=0}^{p-1} \sum_{x,y=L+1}^{L+H} \mathbf{e}_p\left(\lambda\vartheta^x - \lambda\vartheta^y\right) \mathbf{e}_t(bx - by) \\ &= \sum_{x,y=L+1}^{L+H} \mathbf{e}_t\left(b(x-y)\right) \sum_{\lambda=0}^{p-1} \mathbf{e}_p\left(\lambda\left(\vartheta^x - \vartheta^y\right)\right).\end{aligned}$$

Applying Lemma 1 to the inner sum, we obtain the desired identity. □

Let a_1, a_2, a_3, a_4 be fixed integers coprime to p, and as before let L, H be integers with $1 \le H \le t$. For arbitrary divisors d_1, d_2 of t we denote by $Q^{=}_{d_1,d_2}(L, H)$ the number of solutions to the system

$$a_1\vartheta^{x_1} + a_2\vartheta^{x_2} + a_3\vartheta^{x_3} + a_4\vartheta^{x_4} \equiv 0 \pmod p,$$

$$x_1 \equiv x_3 \pmod{d_1}, \qquad x_2 \equiv x_4 \pmod{d_2},$$

$$L + 1 \le x_1, x_2, x_3, x_4 \le L + H,$$

and by $Q^{>}_{d_1,d_2}(L, H)$ the number of solutions to the system

$$a_1\vartheta^{x_1} + a_2\vartheta^{x_2} + a_3\vartheta^{x_3} + a_4\vartheta^{x_4} \equiv 0 \pmod p,$$

$$x_1 \equiv x_3 \pmod{d_1}, \qquad x_2 \equiv x_3 \pmod{d_2},$$

$$L + 1 \le x_1, x_2, x_3, x_4 \le L + H.$$

Then we have the following elementary upper bound:

Lemma 4. *With the above notation, for any $1 \le H \le t$ and any divisors d_1, d_2 of t we have*

$$\max\left\{Q^{=}_{d_1,d_2}(L, H),\, Q^{>}_{d_1,d_2}(L, H)\right\} \ll H^3/d_1d_2 + H^2.$$

Proof. Indeed, to obtain the bound for $Q^{=}_{d_1,d_2}(L, H)$ we begin by counting those solutions for which

$$a_1\vartheta^{x_1} + a_3\vartheta^{x_3} \equiv 0 \equiv a_2\vartheta^{x_2} + a_4\vartheta^{x_4} \pmod p.$$

Here each value of x_1 gives rise to at most one value of x_3 (since $1 \le H \le t$), and each value of x_2 gives rise to at most one value of x_4. Thus there are at most H^2 of these "diagonal" solutions. For the other solutions, where

$$a_1\vartheta^{x_1} + a_3\vartheta^{x_3} \equiv \eta \equiv -(a_2\vartheta^{x_2} + a_4\vartheta^{x_4}) \pmod p$$

for some $\eta \not\equiv 0 \pmod p$, every choice of x_1, x_3 (there are no more than $H(H/d_1+1)$ such choices) determines a nonzero class for $\vartheta^{x_2}(a_2 + a_4\vartheta^{x_4-x_2})$. Once we specify $x_4 - x_2$ (there are no more than $2H/d_2+1$ ways to do this) the rest is determined. Thus,

$$Q^{=}_{d_1,d_2}(L,H) \le H(H/d_1+1)(2H/d_2+1) + H^2 \ll H^3/d_1d_2 + H^2.$$

The bound for $Q^{>}_{d_1,d_2}(L,H)$ is even easier. We see that

$$Q^{>}_{d_1,d_2}(L,H) \le H(H/d_1+1)(H/d_2+1) \ll H^3/d_1d_2 + H^2.$$

□

For small values of d_1, d_2 one can improve on the above result via exponential sums.

Lemma 5. *With the notation as above, for any $1 \le H \le t$ and any divisors d_1, d_2 of t the bounds*

$$Q^{=}_{d_1,d_2}(L,H) = \frac{H^4}{d_1d_2p} + O\left(Hp\log^2 p\right)$$

and

$$Q^{>}_{d_1,d_2}(L,H) = \frac{H^4}{d_1d_2p} + O\left(Hp\log^2 p\right)$$

hold.

Proof. By Lemma 1 we have the exponential sum representation:

$$Q^{=}_{d_1,d_2}(L,H) = \frac{1}{p}\sum_{\lambda=0}^{p-1} \sum_{\substack{x_1,x_2,x_3,x_4=L+1 \\ x_1\equiv x_3 \pmod{d_1} \\ x_2\equiv x_4 \pmod{d_2}}}^{L+H} \mathbf{e}_p\left(\lambda(a_1\vartheta^{x_1} + a_2\vartheta^{x_2} + a_3\vartheta^{x_3} + a_4\vartheta^{x_4})\right).$$

The contribution from terms with $\lambda = 0$ is equal to Tp^{-1}, where T is the number of solutions to the system

$$x_1 \equiv x_3 \pmod{d_1}, \quad x_2 \equiv x_4 \pmod{d_2}, \quad L+1 \le x_1, x_2, x_3, x_4 \le L+H.$$

Thus,

$$\begin{aligned} T &= H^2(H/d_1 + O(1))(H/d_2 + O(1)) \\ &= H^4/d_1d_2 + O(H^3/d_1 + H^3/d_2 + H^2) \\ &= H^4/d_1d_2 + O(H^3) = H^4/d_1d_2 + O\left(Hp^2 \log^2 p\right). \end{aligned}$$

For the rest of the sum, which we denote by R, we have

$$\begin{aligned} R &= \frac{1}{p}\sum_{\lambda=1}^{p-1} \sum_{\substack{x_1,x_2,x_3,x_4=L+1 \\ x_1\equiv x_3 \pmod{d_1} \\ x_2 \equiv x_4 \pmod{d_2}}}^{L+H} \mathbf{e}_p\left(\lambda(a_1\vartheta^{x_1} + a_2\vartheta^{x_2} + a_3\vartheta^{x_3} + a_4\vartheta^{x_4})\right) \\ &= \frac{1}{p}\sum_{\lambda=1}^{p-1} \sum_{x_1,x_2,x_3,x_4=L+1}^{L+H} \mathbf{e}_p\left(\lambda(a_1\vartheta^{x_1} + a_2\vartheta^{x_2} + a_3\vartheta^{x_3} + a_4\vartheta^{x_4})\right) \\ &\qquad \times \frac{1}{d_1d_2}\sum_{b_1=1}^{d_1} e_{d_1}\left(b_1(x_1-x_3)\right) \sum_{b_2=1}^{d_2} e_{d_2}\left(b_2(x_2-x_4)\right) \\ &= \frac{1}{d_1d_2p}\sum_{b_1=1}^{d_1}\sum_{b_2=1}^{d_2}\sum_{\lambda=1}^{p-1} \sigma_1(\lambda a_1, tb_1/d_1; L, H)\sigma_1(\lambda a_2, tb_2/d_2; L, H) \\ &\qquad \times \sigma_1(\lambda a_3, -tb_1/d_1; L, H)\sigma_1(\lambda a_4, -tb_2/d_2; L, H). \end{aligned}$$

To two of the sums, say $\sigma_1(\lambda a_3, -tb_1/d_1; L, H)$ and $\sigma_1(\lambda a_4, -tb_2/d_2; L, H)$, we apply the bound of Lemma 2 and then apply the Cauchy inequality:

$$\begin{aligned} R &\ll \frac{(p^{1/2}\log p)^2}{d_1 d_2 p} \sum_{b_1=1}^{d_1}\sum_{b_2=1}^{d_2}\sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_1, tb_1/d_1; L, H)|\,|\sigma_1(\lambda a_2, tb_2/d_2; L, H)| \\ &\le \frac{\log^2 p}{d_1 d_2} \sum_{b_1=1}^{d_1}\sum_{b_2=1}^{d_2} \left(\sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_1, tb_1/d_1; L, H)|^2\right)^{1/2} \\ &\qquad\qquad \times \left(\sum_{\lambda=1}^{p-1} |\sigma_1(\lambda a_2, tb_2/d_2; L, H)|^2\right)^{1/2} \\ &\le \frac{\log^2 p}{d_1 d_2} \sum_{b_1=1}^{d_1}\sum_{b_2=1}^{d_2} \left(\sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, tb_1/d_1; L, H)|^2\right)^{1/2} \\ &\qquad\qquad \times \left(\sum_{\lambda=0}^{p-1} |\sigma_1(\lambda, tb_2/d_2; L, H)|^2\right)^{1/2}. \end{aligned}$$

Using Lemma 3 we obtain the first bound stated in the lemma.

The proof of the second bound is almost identical. □

Next, we need an upper bound for the number of zeros of exponential equations over a finite field. The one given here improves that used in [**5**] (see Lemma 9 therein), the original version of which dates back to [**17**] .

Lemma 6. *Fix $n \ge 2$, and let $a_1, \ldots, a_n, \vartheta_1, \ldots, \vartheta_n \in \mathbb{F}^*$ be $2n$ arbitrary nonzero elements of a field $\mathbb{F}$. Let r_{ij} denote the multiplicative order of ϑ_i/ϑ_j, $1 \le i < j \le n$ (and formally set $r_{ij} = \infty$ if ϑ_i/ϑ_j is of infinite order). For $n = 2$ put $\rho = r_{12}$, and for $n \ge 3$ define*

$$\rho = \max_{1 \le k \le n} \min_{\substack{1 \le i < j \le n \\ i \ne k, j \ne k}} r_{ij}.$$

Then the number $T(N)$ of solutions of the equation

$$a_1\vartheta_1^x + \ldots + a_n\vartheta_n^x = 0, \qquad 1 \le x \le N,$$

satisfies the bound

$$T(N) \le \left(\tfrac{15}{4}\right)^{n-2} N \left(N^{-1/(n-1)} + \rho^{-1/(n-1)}\right).$$

Proof. We prove the bound by induction on n, the initial case $n = 2$ being trivial.

Now suppose that $n \geq 3$ and that the result holds for all exponential equations with no more than $n - 1$ terms.

Clearly we may assume that $T(N) \geq (\frac{15}{4})^{n-2}$ since otherwise the bound is trivial. After reindexing if necessary, we may also assume that

$$\rho = \min_{1 \leq i < j \leq n-1} r_{ij} \,.$$

Consider the set $\mathcal{M}$ of all ordered $(n-1)$-tuples $(x_1, \ldots, x_{n-1})$ of distinct solutions to the equation in the statement of the lemma; clearly,

$$\#\mathcal{M} = T(N)(T(N) - 1) \ldots (T(N) - (n-2)).$$

For each $(n-1)$-tuple $(x_1, \ldots, x_{n-1}) \in \mathcal{M}$ we define the matrix

$$I(x_1, \ldots, x_{n-1}) = \left(\vartheta_i^{x_j}\right)_{i,j=1}^{n-1}$$

and split $\mathcal{M}$ into two disjoint subsets:

- $\mathcal{M}_1$, the set of $(n-1)$-tuples $(x_1, \ldots, x_{n-1}) \in \mathcal{M}$ which satisfy the condition $\det I(x_1, \ldots, x_{n-1}) = 0$;
- $\mathcal{M}_2$, the set of all other $(n-1)$-tuples in $\mathcal{M}$.

To estimate $\#\mathcal{M}_1$ we remark that the condition $\det I(x_1, \ldots, x_{n-1}) = 0$ gives rise to an $(n-1)$-term exponential equation in x_{n-1}:

$$A_1(x_1, \ldots, x_{n-2})\vartheta_1^{x_{n-1}} + \ldots + A_{n-1}(x_1, \ldots, x_{n-2})\vartheta_{n-1}^{x_{n-1}} = 0, \tag{2·2}$$

where the coefficients $A_1(x_1, \ldots, x_{n-2}), \ldots, A_{n-1}(x_1, \ldots, x_{n-2})$ depend only on the values $x_1, \ldots, x_{n-2}$. In particular, we see that

$$A_{n-1}(x_1, \ldots, x_{n-2}) = I(x_1, \ldots, x_{n-2}).$$

If $I(x_1,\dots,x_{n-2}) \neq 0$, then by induction x_{n-1} can take at most

$$\left(\tfrac{15}{4}\right)^{n-3} N\left(N^{-1/(n-2)} + \rho^{-1/(n-2)}\right)$$

distinct values, while there are at most $T(N)^{n-2}$ possible values for the other variables $x_1,\dots,x_{n-2}$. Thus, the number of solutions $(x_1,\dots,x_{n-1})$ to (2·2) is at most

$$\left(\tfrac{15}{4}\right)^{n-3} T(N)^{n-2} N\left(N^{-1/(n-2)} + \rho^{-1/(n-2)}\right)$$

when $I(x_1,\dots,x_{n-2}) \neq 0$.

Similarly, the condition $I(x_1,\dots,x_{n-2}) = 0$ gives rise to an $(n-2)$-term equation for x_{n-2} with one of the coefficients equal to $I(x_1,\dots,x_{n-3})$. If $I(x_1,\dots,x_{n-3}) \neq 0$ then by induction there are at most

$$\left(\tfrac{15}{4}\right)^{n-4} N\left(N^{-1/(n-3)} + \rho^{-1/(n-3)}\right)$$

possibilities for x_{n-2} and at most $T(N)^{n-2}$ possible values for the remaining variables. However, if $I(x_1,\dots,x_{n-3}) = 0$ then we obtain an $(n-3)$-term equation for x_{n-3}. Continuing in this manner, we eventually arrive at the equation $I(x_1,x_2) = 0$. This is equivalent to $\vartheta_1^{x_1-x_2} = \vartheta_2^{x_1-x_2}$ and therefore has at most $(N/\rho + 1)$ solutions for x_1 when all of the other variables are fixed. Putting everything together, we find that

$$\begin{aligned}\#\mathcal{M}_1 &\le T(N)^{n-2} \sum_{j=2}^{n-1} \left(\tfrac{15}{4}\right)^{j-2} N\left(N^{-1/(j-1)} + \rho^{-1/(j-1)}\right)\\ &< \tfrac{4}{11}\left(\tfrac{15}{4}\right)^{n-2} T(N)^{n-2} N\left(N^{-1/(n-1)} + \rho^{-1/(n-1)}\right).\end{aligned}$$

We now turn our attention to the set $\mathcal{M}_2$. We claim that for each choice of a fixed $(n-2)$-tuple $(z_1,\dots,z_{n-2})$ with $|z_j| \in [1,N], j = 1,\dots,n-2$, the number of $(n-1)$-tuples $(x_1,\dots,x_{n-1}) \in \mathcal{M}_2$ with $z_j = x_j - x_{n-1}$, $j = 1,\dots,n-2$, is at most $N/\rho + 1$. Indeed, putting $z_{n-1} = 0$, we obtain the following system of equations for x_{n-1}:

$$a_1\vartheta_1^{z_j}\vartheta_1^{x_{n-1}} + \ldots + a_{n-1}\vartheta_{n-1}^{z_j}\vartheta_{n-1}^{x_{n-1}} = -a_n\vartheta_n^{z_j}\vartheta_n^{x_{n-1}}, \quad j = 1,\dots,n-1. \qquad (2·3)$$

Since $(x_1,\dots,x_{n-1}) \in \mathcal{M}_2$, we have

$$\det\left(\vartheta_i^{z_j}\right)_{i,j=1}^{n-1} = (\vartheta_1\dots\vartheta_{n-1})^{-x_{n-1}} \det I(x_1,\dots,x_{n-1}) \neq 0.$$

Therefore, by the Cramer rule we see that (2·3) implies that

$$\vartheta_i^{x_{n-1}} + B_i(z_1,\dots,z_{n-2})\vartheta_n^{x_{n-1}} = 0, \qquad i = 1,\dots,n-1,$$

with some coefficients $B_i(z_1,\dots,z_{n-2})$, $i=1,\dots,n-1$, depending only on $z_1,\dots,z_{n-2}$. Thus, for each fixed $(n-2)$-tuple $(z_1,\dots,z_{n-2})$ there are at most $N/\rho+1$ possible values for x_{n-1} after which $x_1,\dots,x_{n-2}$ are uniquely determined. Consequently,

$$\#\mathcal{M}_2 \le (2N)^{n-2}(N/\rho+1).$$

Recalling that $T(N) \ge \left(\frac{15}{4}\right)^{n-2}$, we now estimate

$$\begin{aligned}\#\mathcal{M} &= T(N)(T(N)-1)\dots(T(N)-(n-2))\\ &\ge T(N)^{n-1}\left(1-\frac{n-2}{\left(\frac{15}{4}\right)^{n-2}}\right)^{n-2} \ge \tfrac{8}{11}\,T(N)^{n-1},\end{aligned}$$

the last inequality being valid for all positive integers n. Combining this result with the above bounds on $\#\mathcal{M}_1$ and $\#\mathcal{M}_2$, we derive the inequality

$$\begin{aligned}T(N)^{n-1} &\le \tfrac{11}{8}\#\mathcal{M} = \tfrac{11}{8}(\#\mathcal{M}_1 + \#\mathcal{M}_2)\\ &\le \tfrac{1}{2}(\tfrac{15}{4})^{n-2}\,T(N)^{n-2}N\left(N^{-1/(n-1)} + \rho^{-1/(n-1)}\right) + \tfrac{11}{8}\,(2N)^{n-2}(N/\rho+1)\end{aligned}$$

Thus we have either

$$T(N)^{n-1} \le (\tfrac{15}{4})^{n-2}\,T(N)^{n-2}N\left(N^{-1/(n-1)} + \rho^{-1/(n-1)}\right)$$

or

$$T(N)^{n-1} \le \tfrac{11}{4}(2N)^{n-2}(N/\rho+1).$$

Noting that, in the latter case,

$$\left(\tfrac{11}{4}\cdot 2^{n-2}\right)^{1/(n-1)} < \left(\tfrac{15}{4}\right)^{n-2}$$

for all $n \ge 3$, the result follows. □

As usual, we denote by $\tau(m)$ the number of positive integral divisors of $m \ge 1$:

$$\tau(m) = \sum_{d\,|\,m} 1.$$

For any fixed $\varepsilon > 0$, we have the following well-known estimate:

$$\tau(m) = O(m^{\varepsilon}), \tag{2·4}$$

where the implied constant in the Landau symbol depends only on ε; see for example exercise 11.c in Chapter 2 of [**19**].

3. *Main Results*

Theorem 7. *Let $\mathcal{X}$ and $\mathcal{Y}$ be intervals of the form $\mathcal{X} = [L+1, L+H]$, $\mathcal{Y} = [M+1, M+K]$ with $1 \le H, K \le t$. Then for any integers a, c such that $\gcd(ac,p) = 1$ the following bound holds:*

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll \left(H^{16/5}K^{11/15}p^{4/5} + H^{16/15}Kt^{-4/15}p^{34/15}\right)\tau(t)^{8/5}\log^{8/5} p.$$

Proof. It is clear that the bound is nontrivial only if

$$H^{16/5}K^{11/15}p^{4/5} \le KH^4$$

which is equivalent to the inequality $H^4K^{4/3} \ge p^4$; since $K \le t < p$, we may therefore assume without loss of generality that $H \ge p^{2/3}$.

Let us introduce a positive integer parameter h to be chosen later. We claim that

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll h^{-1}\sum_{y\in\mathcal{Y}}\sum_{\lambda,\mu=0}^{p-1}\left|\sum_{x\in\mathcal{X}} \mathbf{e}_p\left(\lambda\vartheta^x + \mu\vartheta^{xy}\right)\right|^4 + Kh^4.$$

Note that if $h > H$ this follows from the trivial bound $V_{a,c}(\mathcal{X},\mathcal{Y}) \le KH^4$.

To prove the claim in case $h \le H$ (and thus $h \le t$) we argue as in the proof of Theorem 12 of [**5**]. We apply Hölder's inequality twice and make a translation of variables $x \to x+z$, obtaining:

$$\begin{aligned}
V_{a,c}(\mathcal{X},\mathcal{Y}) &= \sum_{y\in\mathcal{Y}} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_p\left(a\vartheta^x + c\vartheta^{xy}\right)\right|^4 \\
&\le \sum_{y\in\mathcal{Y}} \left(\frac{1}{h}\sum_{z=0}^{h-1} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_p\left(a\vartheta^{x+z} + c\vartheta^{(x+z)y}\right)\right| + h\right)^4 \\
&\ll h^{-1}\sum_{y\in\mathcal{Y}}\sum_{z=0}^{h-1} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_p\left(a\vartheta^{z}\vartheta^x + c\vartheta^{zy}\vartheta^{xy}\right)\right|^4 + Kh^4 \\
&\le h^{-1}\sum_{y\in\mathcal{Y}}\sum_{\lambda,\mu=0}^{p-1} \left| \sum_{x\in\mathcal{X}} \mathbf{e}_p\left(\lambda\vartheta^x + \mu\vartheta^{xy}\right)\right|^4 + Kh^4
\end{aligned}$$

since, for each fixed $y \in \mathcal{Y}$, the pairs $(a\vartheta^z, c\vartheta^{zy})$, $z = 0,\ldots,h-1$, are all necessarily distinct modulo p due to the inequality $h \le t$. Using Lemma 1 it follows that

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll h^{-1}p^2T + Kh^4, \qquad (3\cdot1)$$

where T is the number of solutions (x_1,x_2,x_3,x_4,y) to the system

$$\begin{gathered}
\vartheta^{x_1} + \vartheta^{x_2} \equiv \vartheta^{x_3} + \vartheta^{x_4} \pmod p, \\
\vartheta^{x_1y} + \vartheta^{x_2y} \equiv \vartheta^{x_3y} + \vartheta^{x_4y} \pmod p, \\
x_1,x_2,x_3,x_4 \in \mathcal{X}, \qquad y \in \mathcal{Y}.
\end{gathered}$$

Using Lemma 6 with $n = 4$ we see that, for each fixed quadruple (x_1,x_2,x_3,x_4), there are at most

$$N_d \le 15K(K^{-1/3} + t^{-1/3}d^{1/3})$$

values of $y \in \mathcal{Y}$ which satisfy that system, where

$$d = \min_{1\le k\le 4}\max_{\substack{1\le i<j\le 4\\ i\ne k, j\ne k}} \gcd(x_i - x_j, t). \qquad (3\cdot2)$$

We fix a divisor d of t and denote by M_d the number of quadruples (x_1, x_2, x_3, x_4) for which (3·2) holds. The condition (3·2) implies that there is a permutation $\{i_1, i_2, i_3, i_4\}$ of the set $\{1, 2, 3, 4\}$ such that

$$\gcd(x_{i_1} - x_{i_3}, t) = d_1 \qquad \gcd(x_{i_2} - x_{i_4}, t) = d_2$$

or else such that

$$\gcd(x_{i_1} - x_{i_3}, t) = d_1 \qquad \gcd(x_{i_2} - x_{i_3}, t) = d_2$$

for two divisors d_1, d_2 of t with $\min\{d_1, d_2\} = d$. (In the latter case we can also assert that $\gcd(x_{i_1} - x_{i_2}, t) = d_3$ for a third divisor $d_3 \geq d$ but this is unnecessary.) Thus, for each fixed d there are at most $2\tau(t)$ suitable pairs (d_1, d_2). Using Lemmas 4 and 5 we deduce that

$$M_d \ll \min\left\{H^3/d^2 + H^2, H^4/d^2p + Hp\log^2 p\right\}\tau(t).$$

We now substitute the above bounds in the inequality

$$T \leq \sum_{d \mid t} M_d N_d,$$

and choose optimally between the bounds for M_d, namely using the first inequality for $d > B$ and the second for $d \leq B$, where $B = Hp^{-1/2}\log^{-1} p$. This yields the estimate

$$T \ll (\Sigma_1 + \ldots + \Sigma_8)\,\tau(t),$$

where

$$\begin{aligned}
\Sigma_1 &= H^4K^{2/3}p^{-1}\sum_{\substack{d\,|\,t\\ d\le B}} d^{-2},\\
\Sigma_2 &= HK^{2/3}p\log^2 p\sum_{\substack{d\,|\,t\\ d\le B}} 1,\\
\Sigma_3 &= H^4Kt^{-1/3}p^{-1}\sum_{\substack{d\,|\,t\\ d\le B}} d^{-5/3},\\
\Sigma_4 &= HKt^{-1/3}p\log^2 p\sum_{\substack{d\,|\,t\\ d\le B}} d^{1/3},
\end{aligned}$$

and

$$\begin{aligned}
\Sigma_5 &= H^3K^{2/3}\sum_{\substack{d\,|\,t\\ d> B}} d^{-2},\\
\Sigma_6 &= H^2K^{2/3}\sum_{\substack{d\,|\,t\\ d> B}} 1,\\
\Sigma_7 &= H^3Kt^{-1/3}\sum_{\substack{d\,|\,t\\ d> B}} d^{-5/3},\\
\Sigma_8 &= H^2Kt^{-1/3}\sum_{\substack{d\,|\,t\\ d> B}} d^{1/3}.
\end{aligned}$$

Using elementary estimates we obtain that

$$\begin{aligned}
&\Sigma_1, \Sigma_3 \ll \tau(t)H^4K^{2/3}p^{-1},\\
&\Sigma_2, \Sigma_5 \ll \tau(t)HK^{2/3}p\log^2 p,\\
&\Sigma_4, \Sigma_7 \ll \tau(t)H^{4/3}Kt^{-1/3}p^{5/6}\log^{5/3} p,\\
&\Sigma_6, \Sigma_8 \ll \tau(t)H^2K.
\end{aligned}$$

Combining the above estimates we bound T by

$$T \ll \left(H^4K^{2/3}p^{-1} + HK^{2/3}p + H^{4/3}Kt^{-1/3}p^{5/6} + H^2K\right)\tau(t)^2\log^2 p.$$

On the other hand, the inequality

$$H^4K^{2/3}p^{-1} < HK^{2/3}p$$

is equivalent to $H < p^{2/3}$; thus it is never satisfied. Similarly, the inequality

$$H^4K^{2/3}p^{-1} < H^2K$$

is equivalent to $H^2 < K^{1/3}p$, and this is less than $p^{4/3}$ which is also not possible for $H \geq p^{2/3}$. Therefore

$$T \ll \left(H^4K^{2/3}p^{-1} + H^{4/3}Kt^{-1/3}p^{5/6}\right)\tau(t)^2\log^2 p.$$

Inserting this bound in (3·1) and then optimising with the choice

$$h = \left\lfloor \left(H^{4/5}K^{-1/15}p^{1/5} + H^{4/15}t^{-1/15}p^{17/30}\right)\tau(t)^{2/5}\log^{2/5} p\right\rfloor,$$

we conclude the proof. □

The special cases where $\gcd(ac,p) \neq 1$ are not covered by the above theorem. For completeness, we give results for these as well. Of course, if both a and c are divisible by p then there can be no nontrivial bound. In the other cases we have:

Theorem 8. *Suppose that* $\gcd(a,c,p) = 1$ *but* $\gcd(ac,p) \neq 1$. *Assume that* $p^{1/2}\log p \leq H, K \leq t$. *Then*

- *if* $a \equiv 0 \pmod p$ *we have*

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll H^4Kt^{-1}\tau(t)p^{1/2}\log p + K\tau(t)p^2\log^4 p$$

- *while if* $c \equiv 0 \pmod p$ *we have*

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll Kp^2\log^4 p.$$

Proof. If $a \equiv 0 \pmod p$ then $c \not\equiv 0 \pmod p$, and we have

$$V_{a,c}(\mathcal{X},\mathcal{Y}) = \sum_{d \mid t} \sum_{\substack{y \in Y \\ \gcd(y,t)=d}} \left| \sum_{x \in \mathcal{X}} \mathbf{e}_p\left(c\vartheta^{xy}\right) \right|^4 = \sum_{d \mid t} \sum_{\substack{y \in Y \\ \gcd(y,t)=d}} |\sigma_y(c,0;L,H)|^4 .$$

Let $s \le K$ be a positive integer parameter to be chosen later. For the large divisors, with $d > s$, we apply the trivial estimate $|\sigma_y(c,0;L,H)| \le H$, obtaining the bound

$$\sum_{\substack{d \mid t \\ d>s}} \sum_{\substack{y \in Y \\ \gcd(y,t)=d}} |\sigma_y(c,0;L,H)|^4 \ll H^4 \sum_{\substack{d \mid t \\ d>s}} (K/d+1) < H^4(Ks^{-1}+1)\tau(t).$$

For the smaller divisors, we apply (2·1) and find that

$$\begin{aligned} \sum_{\substack{d \mid t \\ d \le s}} \sum_{\substack{y \in Y \\ \gcd(y,t)=d}} |\sigma_y(c,0;L,H)|^4 &\ll \sum_{\substack{d \mid t \\ d \le s}} \sum_{\substack{y \in Y \\ \gcd(y,t)=d}} \left(\frac{d^4H^4}{t^4}+1\right) p^2 \log^4 p \\ &\ll p^2 \log^4 p \sum_{\substack{d \mid t \\ d \le s}} \left(\frac{d^4H^4}{t^4}+1\right)(K/d) \\ &\ll \left(H^4 t^{-4} s^3 + 1\right) K\tau(t) p^2 \log^4 p. \end{aligned}$$

We choose $s = tp^{-1/2}\log^{-1} p$ to optimise and note that, for this choice, we necessarily have $1 \le s < K$. The result follows in this case.

If $c \equiv 0 \pmod p$ then $a \not\equiv 0 \pmod p$, and the result in this case follows immediately from Lemma 2. □

4. *Remarks*

We draw attention to some interesting special cases of Theorem 7. Let us take ϑ to be a primitive root modulo p (that is, $t = p-1$), and assume that $\gcd(ac,p) = 1$. First of all, if the sum over x is complete (that is, $\mathcal{X} = [1,p-1]$) then we obtain from Theorem 7 (noting that the second term never dominates in this case) the bound

$$V_{a,c}(\mathcal{X},\mathcal{Y}) \ll K^{11/15} p^4 \tau(p-1)^{8/5} \log^{8/5} p,$$

which by (2·4) is nontrivial for any $K \ge p^{\varepsilon}$. Actually though, as we shall see very soon, this particular case can be improved.

On the other hand, if the sum over y is complete (that is, $\mathcal{Y} = [1, p-1]$) then we obtain from Theorem 7 that

$$V_{a,c}(\mathcal{X}, \mathcal{Y}) \ll \left(H^{16/5}p^{23/15} + H^{16/15}p^{3}\right)\tau(p-1)^{8/5}\log^{8/5} p,$$

which is nontrivial for $H \ge p^{15/22+\varepsilon}$.

Another interesting case occurs when $H = K$, for which we obtain a nontrivial bound provided that $H = K \ge p^{3/4+\varepsilon}$.

In the special case $H = t$, the same method as in Theorem 7 can be used in a sharper fashion to derive the following stronger estimate:

$$\sum_{y=M+1}^{M+K} \left|\sum_{x=1}^{t} \mathbf{e}_p\left(a\vartheta^{x} + c\vartheta^{xy}\right)\mathbf{e}_t\left(\alpha x\right)\right|^4 < \left(K^{2/3}t^{3}p + Kp^{17/6}\right)p^{o(1)}. \qquad (4·1)$$

This bound is a generalization of Theorem 8 of [**4**] which dealt with the case $K = t$, $\alpha = 0$. The method of [**4**] would extend to give this result for arbitrary α but not for general $K < t$.

Indeed, one sees that if $\mathcal{X} = [1, t]$ then, by periodicity, the translations $x \to x + z$, made in the proof of Theorem 7 do not lead to the additional term $O(h)$, so we simply have

$$\sum_{x=1}^{t} \mathbf{e}_p\left(a\vartheta^{x} + c\vartheta^{xy}\right)\mathbf{e}_t\left(\alpha x\right) = h^{-1}\sum_{z=0}^{h-1}\sum_{x=1}^{t} \mathbf{e}_p\left(a\vartheta^{x+z} + c\vartheta^{(x+z)y}\right)\mathbf{e}_t\left(\alpha(x+z)\right),$$

for each y and for any h. Thus the term Kh^4 does not appear in the corresponding version of (3·1). It is easy to see that the "weight" $\mathbf{e}_t\left(\alpha x\right)$ does not change the shape of that bound; the parameter T will count the solutions of the same system as before.

This enables us to take the largest admissible value $h = t$ and thus simple calculations lead to the estimate (4·1). By Hölder's inequality and the well–known method of completing the sum (see for example [**6**]), this bound (4·1) immediately leads to the same upper bound for incomplete sums $V_{a,c}(\mathcal{X},\mathcal{Y})$ over intervals of the form $\mathcal{X} = [L+1, L+H]$, $\mathcal{Y} = [M+1, M+K]$:

$$V_{a,c}(\mathcal{X},\mathcal{Y}) < \left(K^{2/3}t^3p + Kp^{17/6}\right)p^{o(1)} \tag{4·2}$$

provided that $\gcd(ac, p) = 1$. For some values of the parameters this bound is stronger than the bound of Theorem 7; in particular, this is true when the sum is nearly complete over both x and y. Thus, for example, in the case $t = p-1$, $H = K$, this bound is stronger for $K \geq p^{48/49+\varepsilon}$.

It is easily seen that in the proof of Theorem 7 the combinatorics involving the divisors d of the order t are greatly simplified in the case that t is prime. However this does not allow for any improvements in the result.

In many places throughout we have been somewhat relaxed with estimates for sums over divisors and hence there are available some tiny improvements of size $p^{o(1)}$.

All of the results of this paper extend without new arguments to the case where the prime field of residue classes modulo p is replaced by any finite field of $q = p^m$ elements and the exponential $\mathbf{e}_p$ is replaced by any nontrivial additive character of the field. The bounds given above hold just as stated but with p replaced by q throughout.

Bourgain [**3**] has recently shown how to bound the sum $S_{a,b,c}(\mathcal{X},\mathcal{Y})$ nontrivially for *any* $H \geq p^{\varepsilon}$, $K \geq p^{\varepsilon}$, provided that $\gcd(a, b, c, p) = 1$. Although these bounds are not as explicit as those implied by Theorem 7 for the cases considered here, his estimates remain nontrivial over remarkably short intervals. It would be very interesting to know the explicit exponents achievable by Bourgain's method and also to have an extension of the arguments to the case of an arbitrary finite field with $q = p^m$ elements.

REFERENCES

[**1**] W. Banks, A. Conflitti, J. B. Friedlander and I. E. Shparlinski. Exponential sums over Mersenne numbers. *Compositio Math.* **140** (2003) 15–30.

[**2**] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices Amer. Math. Soc.* **46** (1999) 203–213.

[**3**] J. Bourgain. Estimates on exponential sums related to the Diffie-Hellman distributions. *Comptes Rendus Mathematique* **338** (2004) 825-830.

[**4**] R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman and I. E. Shparlinski. On the statistical properties of Diffie–Hellman distributions. *Israel J. Math.* **120** (2000) 23–46.

[**5**] R. Canetti, J. B. Friedlander and I. E. Shparlinski. On certain exponential sums and the distribution of Diffie–Hellman triples. *J. London Math. Soc.* **59** (1999) 799–812.

[**6**] J. H. H. Chalk. The Vinogradov–Mordell–Tietäväinen inequalities. *Indag. Math.* **42** (1980) 367–374.

[**7**] J. B. Friedlander, J. Hansen and I. E. Shparlinski. On the distribution of the power generator modulo a prime power. *Proc. DIMACS Workshop on Unusual Applications of Number Theory, 2000*, Amer. Math. Soc., 2004, 71–79.

[**8**] J. B. Friedlander, S. V. Konyagin and I. E. Shparlinski. Some doubly exponential sums over $\mathbb{Z}_m$. *Acta Arith.* **105** (2002) 349–370.

[**9**] J. B. Friedlander, D. Lieman and I. E. Shparlinski. On the distribution of the RSA generator. *Proc. Intern. Conf. on Sequences and their Applications, Singapore 1998.* (Springer-Verlag, London, 1999) 205–212.

[**10**] J. B. Friedlander and I. E. Shparlinski. On the distribution of Diffie–Hellman triples with sparse exponents. *SIAM J. Discr. Math.* **14** (2001) 162–169.

[**11**] E. Kiltz. On the representation of Boolean predicates of the Diffie–Hellman function. *Preprint* (2002) 1–17.

[**12**] S. V. Konyagin and I. Shparlinski. *Character sums with exponential functions and their applications*. (Cambridge Univ. Press, Cambridge, 1999).

[**13**] N. M. Korobov. On the distribution of digits in periodic fractions. *Math. USSR – Sbornik* **18** (1972) 659–676.

[**14**] N. M. Korobov. *Exponential sums and their applications*. (Kluwer Acad. Publ., North-Holland, 1992).

[**15**] R. Lidl and H. Niederreiter. *Finite fields.* (Addison-Wesley, MA, 1983).

[**16**] H. Niederreiter. Quasi-Monte Carlo methods and pseudo-random numbers. *Bull. Amer. Math. Soc.* **84** (1978) 957–1041.

[**17**] I. E. Shparlinski. On prime divisors of recurrence sequences. *Izvestija Vysshih Uchebnyh Zavedenii, Ser. matem.* (1980) no.1, 100–103 (in Russian).

[**18**] I. E. Shparlinski. Communication complexity and Fourier coefficients of the Diffie–Hellman key. *Lect. Notes in Comp. Sci.* (Springer-Verlag, Berlin, **1776**, 2000) 259–268.

[**19**] I. M. Vinogradov. *Elements of number theory.* (Dover Publ., NY, 1954).