ON THE DISTRIBUTION OF ORBITS OF $\text{PGL}_2(q)$ IN $\mathbb{F}_q^n$ AND THE KLAPPER CONJECTURE*

IGOR E. SHPARLINSKI†

Abstract. Motivated by a conjecture of Klapper [Finite Fields, Coding Theory, and Advances in Communications and Computing, Marcel Dekker, New York, 1993], we study the distribution of elements $\xi$ of a finite field $\mathbb{F}_q^n$ of $q^n$ elements under the action of the transformations $\xi \mapsto (a\xi + b)/(c\xi + d)$ for matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(q)$. We slightly improve a result of Niederreiter and Winterhof [Finite Fields Appl., 9 (2003), pp. 458–471] towards this conjecture. On the other hand, we also show that the original conjecture is false as stated.

Key words. Klapper conjecture, $\text{PGL}_2(q)$ orbits, character sums

AMS subject classifications. 11L40, 11T30

DOI. 10.1137/090770746

1. Introduction. Given an element $\xi$ which is a root of an irreducible polynomial of degree $n$ over a finite field $\mathbb{F}_q$ of $q$ elements, that is, such that $\mathbb{F}_q(\xi) = \mathbb{F}_{q^n}$, we consider its orbit

$$\text{Orb}(\xi) = \left\{ (a\xi + b)/(c\xi + d) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(q) \right\}$$

associated with matrices from the projective general linear group $\text{PGL}_2(q)$ over $\mathbb{F}_q$.

For a fixed primitive element $\gamma$ of $\mathbb{F}_q^n$ and integers $h \geq 0$ and $k \geq 1$, we denote by $T_\xi(h, k)$ the number of elements of $\text{Orb}(\xi)$ which are also of the form $\gamma^h + i$ for some $i = 0, \ldots, k - 1$, that is,

$$T_\xi(h, k) = \# \left( \text{Orb}(\xi) \cap \{ \gamma^h, \ldots, \gamma^{h+k-1} \} \right).$$

Finding good estimates on $T_\xi(h, k)$ is important for studying the autocorrelation of so-called geometric sequences of pseudorandom numbers; see [2, 3] for this connection and some upper bounds on $T_\xi(h, k)$.

In particular, Klapper [2] has made the following conjecture.

CONJECTURE 1. There exists an absolute constant $C > 0$ such that if $k \geq (q^n - 1)/(q^3 - 1)$, then

$$T_\xi(h, k) \leq Ckq^{-n+3}.$$

Motivated by this conjecture, Niederreiter and Winterhof [5, Theorem 1] have shown that the bound of Conjecture 1 holds for

$$k > n^3q^{n-2}\log q,$$

which in particular improves the previous estimate of [3, Proposition 15]; see also [5, Proposition 1].

*Received by the editors September 10, 2009; accepted for publication (in revised form) October 6, 2009; published electronically January 15, 2010. This work was supported in part by ARC grant DP0556431.

†Department of Computing, Macquarie University, Sydney, NSW 2109, Australia (igor@comp.mq.edu.au).
Here we show that the same bound holds starting with slightly smaller values of $k$.

On the other hand, we show that Conjecture 1 is false, and its bound may have a chance to be true starting only with larger values of $k$.

Although our approach can be made uniform with respect to both $q$ and $n$, to simplify the exposition, we always assume that $n$ is fixed. In particular, the implied constants in the symbols “$O$”, “$≪$”, and “$≫$” are always absolute. We recall that the notations $U = O(V)$, $U ≪ V$, and $V ≫ V$ are all equivalent to the assertion that the inequality $|U| \leq cV$ holds for some constant $c > 0$.

2. Upper bound. Let us fix a multiplicative character $\chi$ of $\mathbb{F}_{q^n}$ of order $q^n - 1$, that is, such that for any positive $d < q^n - 1$ the character $\chi^d$ is nontrivial; see [1, 4] for a background on characters.

We now define the multiplicative character sums along the orbit $\text{Orb}(\xi)$:

$$S_{\xi}(j) = \sum_{\eta \in \text{Orb}(\xi)} \chi^j(\eta),$$

where we also use the standard conventions that $\chi(0) = 0$ and $0^0 = 1$.

Our main tool is the bound of the sums $S_{\xi}(j)$, which is given by Niederreiter and Winterhof [5, Theorem 3].

**Lemma 2.** For any integer $j$ with $0 \leq j \leq q^n - 2$, we have

$$S_{\xi}(j) = \begin{cases} q^3 - q & \text{if } j = 0, \\ 0 & \text{if } j \not\equiv 0 \pmod{q-1}, \end{cases}$$

and

$$|S_{\xi}(j)| < 2(n - 1)^2(q^2 - q)$$

if $j \equiv 0 \pmod{q-1}$ and $j \neq 0$.

**Theorem 3.** For any integer $k \geq 1$ we have

$$T_{\xi}(h, k) \ll kq^{-n+3} + n^2q.$$

**Proof.** Since each $\ell = 0, \ldots, k - 1$ admits at least $k$ representations of the form $\ell = r - s$ with some integers $r, s = 0, \ldots, 2k - 1$, we obtain

$$T_{\xi}(h, k) \leq \frac{1}{k}Q_{\xi}(h, k),$$

where $Q_{\xi}(h, k)$ is the number of solutions to the equation

$$\eta = \gamma^{h+r-s}, \quad \eta \in \text{Orb}(\xi), \quad r, s = 0, \ldots, 2k - 1.$$

By the orthogonality property of characters, for any $\alpha \in \mathbb{F}_{q^n}^*$ we have

$$\frac{1}{q^n - 1} \sum_{j=0}^{q^n - 2} \chi^j(\alpha) = \begin{cases} 1 & \text{if } \alpha = 1, \\ 0 & \text{if } \alpha \neq 1. \end{cases}$$
Therefore,

\[ Q_\xi(h, k) = \sum_{\eta \in \text{Orb}(\xi)} \sum_{r,s=0}^{2k-1} \frac{1}{q^n - 1} \sum_{j=0}^{q^n-2} \chi_j \left( \eta \gamma^{-h-r+s} \right) \]

\[ = \frac{1}{q^n - 1} \sum_{j=0}^{q^n-2} \chi_j \sum_{r,s=0}^{2k-1} \left( \eta \right) \sum_{r,s=0}^{2k-1} \chi_j \left( \gamma^{-h-r+s} \right) \]

\[ = \frac{1}{q^n - 1} \sum_{j=0}^{q^n-2} \chi_j\left(\gamma^{-h}\right) S_\xi(j) \sum_{r,s=0}^{2k-1} \chi_j(\gamma^{s-r}). \]

Separating the term \( S_\xi(0)(2k)^2/(q^n - 1) \) corresponding to \( j = 0 \) and using Lemma 2, we obtain

\[ \left| Q_\xi(h, k) - \frac{4(q^3 - q)k^2}{q^n - 1} \right| \leq \frac{1}{q^n - 1} \sum_{j=0}^{q^n-2} \left| S_\xi(j) \right| \sum_{r,s=0}^{2k-1} \chi_j(\gamma^{s-r}) \]

\[ < \frac{2(n - 1)^2(q^2 - q)}{q^n - 1} \sum_{j=0}^{q^n-2} \left| \sum_{r,s=0}^{2k-1} \chi_j(\gamma^{s-r}) \right|. \]

(4)

Since \( \chi \) is a character of order \( q^n - 1 \), there exists some integer \( a \) with \( \gcd(a, q^n - 1) = 1 \) and such that

\[ \chi(\gamma^u) = \exp \left( 2\pi i \frac{au}{q^n - 1} \right), \]

where \( i = \sqrt{-1} \). Hence,

\[ \sum_{r,s=0}^{2k-1} \chi_j(\gamma^{s-r}) = \sum_{r,s=0}^{2k-1} \exp \left( 2\pi i \frac{ja(s-r)}{q^n - 1} \right) = \sum_{r=0}^{2k-1} \exp \left( 2\pi i \frac{jar}{q^n - 1} \right)^2. \]

Therefore, as the last expression is real positive, we can rewrite (4) as

\[ \left| Q_\xi(h, k) - \frac{4(q^3 - q)k^2}{q^n - 1} \right| \]

\[ < \frac{2(n - 1)^2(q^2 - q)}{q^n - 1} \sum_{j=0}^{q^n-2} \left| \sum_{r=0}^{2k-1} \exp \left( 2\pi i \frac{jar}{q^n - 1} \right) \right|^2. \]

\[ < n^2 q^{-n+2} \sum_{m=1}^{Q-1} \sum_{r=0}^{2k-1} \exp \left( 2\pi i \frac{mar}{Q} \right)^2, \]

where

\[ Q = \frac{q^n - 1}{q - 1}. \]
Further, for any integer \( u \) we have the identity

\[
\frac{1}{Q} \sum_{v=0}^{Q-1} \exp \left( \frac{2\pi i vu}{Q} \right) = \begin{cases} 
1 & \text{if } u \equiv 0 \pmod{Q}, \\
0 & \text{if } u \not\equiv 0 \pmod{Q}.
\end{cases}
\]

Thus, denoting by \( \ell \) the reminder of \( 2k \) on division by \( Q \), we have

\[
\sum_{r=0}^{2k-1} \exp \left( \frac{2\pi i mar}{Q} \right) = \sum_{r=0}^{\ell-1} \exp \left( \frac{2\pi i mar}{Q} \right).
\]

Thus we see from (5) that

\[
Q \xi(h,k) - \frac{4(q^3 - q)k^2}{q^n - 1} \ll n^2 q^{-n+2} \sum_{m=1}^{Q-1} \left| \sum_{r=0}^{\ell-1} \exp \left( \frac{2\pi i mar}{Q} \right) \right|^2.
\]

Now, extending the summation to all \( m = 0, \ldots, Q-1 \) and using (6), we deduce

\[
\sum_{m=1}^{Q-1} \left| \sum_{r=0}^{\ell-1} \exp \left( \frac{2\pi i mar}{Q} \right) \right|^2 \leq Q \sum_{r,s=0}^{\ell-1} \sum_{m=0}^{Q-1} \exp \left( \frac{2\pi i (m+s-r)Q}{Q} \right) = QW,
\]

where \( W \) is the number of solutions to the congruence \( r \equiv s \pmod{Q}, 0 \leq r, s \leq \ell-1 \). Since \( \ell < Q \), this is possible only for \( r = s \). Thus \( W = \ell \), and we obtain

\[
\sum_{m=1}^{Q-1} \left| \sum_{r=0}^{\ell-1} \exp \left( \frac{2\pi i ar}{Q} \right) \right|^2 \leq Q \ell,
\]

which after substitution in (7) implies

\[
Q \xi(h,k) - \frac{4(q^3 - q)k^2}{q^n - 1} \ll n^2 q^{-n+2} Q \ell \ll n^2 q \ell.
\]

In particular, since \( \ell \leq 2k \),

\[
Q \xi(h,k) \ll k^2 q^{-n+3} + n^2 kq.
\]

Recalling (2) we obtain the result. 

In particular, we see from Theorem 3 that the bound of Conjecture 1 holds for

\[
k > n^2 q^{n-2},
\]

which improves on the condition (1) with respect to both \( n \) and \( q \).

### 3. Lower bound.

**Theorem 4.** For any

\[ \alpha < \frac{1}{8} \]

there exists some \( n_0(\alpha) \) such that for any \( q \) and \( n \geq n_0(\alpha) \) there exists \( \xi \in \mathbb{F}_{q^n} \) with \( \mathbb{F}_q(\xi) = \mathbb{F}_{q^n} \) and such that

\[ T_\xi(0,k) \geq an \]

for every \( k \geq (q^n - 1)/(q^3 - 1) \).
Proof. We fix some \( \beta \) with
\[
\alpha < \beta < \frac{1}{8}
\]
and put
\[
m = \lceil \beta n \rceil - 1.
\]
We now fix \( m \) pairwise distinct elements \( b_1, \ldots, b_m \in \mathbb{F}_q^* \) and consider the matrices
\[
\begin{pmatrix}
1 & b_\nu \\
0 & 1
\end{pmatrix}, \quad \nu = 1, \ldots, m,
\]
which are distinct elements of \( \text{PGL}_2(q) \). We now define \( N(k, m) \) as the number of \( \xi \in \mathbb{F}_{q^n} \) such that for every \( \nu = 1, \ldots, m \) we have
\[
\xi + b_\nu = \gamma^{t_\nu}
\]
for some integer \( t_\nu = 0, \ldots, k - 1 \). We also use \( N^*(k, m) \) to denote the number of \( \xi \in \mathbb{F}_{q^n} \), which besides the above conditions also satisfy \( \mathbb{F}_q(\xi) = \mathbb{F}_{q^n} \). It is certainly enough to show that \( N^*(k, m) > 0 \).

Since there are at most \( nq^{n/2} \) elements \( \xi \in \mathbb{F}_{q^n} \) with \( \mathbb{F}_q(\xi) \neq \mathbb{F}_{q^n} \) (they are all in subfields \( \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n} \) with \( d \mid n \) and \( d < n \)), we obtain
\[
N^*(k, m) \geq \frac{1}{\ell m} \left( \frac{nq^n}{q^n - 1} - nq^{n/2} \right).
\]

Let \( \ell = \lceil k/2 \rceil \). Since every \( t = 0, \ldots, k - 1 \) has at most \( \ell \) representations of the form \( t = \ell + r - s \) with \( r, s = 0, \ldots, \ell - 1 \), we see that
\[
N(k, m) \geq \frac{1}{\ell m} M(k, m),
\]
where \( M(k, m) \) is the number of solutions to the system of equations
\[
\xi + b_\nu = \gamma^{\ell + r_\nu - s_\nu},
\]
where
\[
\xi \in \mathbb{F}_{q^n} \quad \text{and} \quad r_\nu, s_\nu = 0, \ldots, \ell - 1, \nu = 1, \ldots, m.
\]
As in the proof of Theorem 3, using (3), we obtain
\[
M(k, m) = \frac{1}{(q^n - 1)^m} \sum_{\xi \in \mathbb{F}_{q^n}} \sum_{r_1, s_1, \ldots, r_m, s_m = 0}^{\ell - 1} \prod_{\nu = 1}^{m} \chi^{j_\nu}(\xi + b_\nu)^{\gamma^{r_\nu - s_\nu}}.
\]
Changing the order of summation and separating the term corresponding to \( j_1 = \cdots = j_m = 0 \), we obtain
\[
\left| M(k, m) - \frac{q^n \ell 2m}{(q^n - 1)^m} \right| \leq \frac{1}{(q^n - 1)^m} \sum_{\xi \in \mathbb{F}_{q^n}} \sum_{\nu = 1}^{m} \prod_{\nu = 1}^{m} \chi^{j_\nu}(\xi + b_\nu) \left| \sum_{j_1, \ldots, j_m = 0}^{\ell - 1} \prod_{\nu = 1}^{m} \chi^{j_\nu}(\gamma^{s_\nu - r_\nu}) \right|.
\]
Applying the Weil bound in the form given in [1, Theorem 11.23] (which depends only on the number of distinct roots of the polynomial argument in the character rather than on its degree) to the sum over $\xi$, we derive

$$\left| \sum_{\xi \in \mathbb{F}_q} \prod_{\nu=1}^{m} \chi^{j_\nu}(\xi + b_\nu) \right| = \left| \sum_{\xi \in \mathbb{F}_q} \chi \left( \prod_{\nu=1}^{m} (\xi + b_\nu)^{j_\nu} \right) \right| \leq mq^{n/2}$$

for any integers $0 \leq j_1, \ldots, j_m \leq q^n - 2$ which are not all zeros (since $\chi$ is of order $q^n - 1$). Therefore,

$$M(k, m) - \frac{q^n \ell 2m}{(q^n - 1)^m} \leq \frac{mq^{n/2}}{(q^n - 1)^m} \sum_{j_1, \ldots, j_m = 0}^{q^n - 2} \prod_{\nu=1}^{m} \sum_{r_\nu, s_\nu = 0}^{\ell - 1} \chi^{j_\nu} (\gamma^{s_\nu - r_\nu}) \leq \frac{mq^{n/2}}{(q^n - 1)^m} \sum_{j_1, \ldots, j_m = 0}^{q^n - 2} \prod_{\nu=1}^{m} \sum_{r_\nu, s_\nu = 0}^{\ell - 1} \chi^{j_\nu} (\gamma^{s_\nu - r_\nu}).$$

Since $k > 1$ for $n \geq 4$ (which we can assume without loss of generality), we have $\ell < k \leq q^n - 1$. Now, again as in the proof of Theorem 3, we derive

$$\sum_{j=0}^{q^n - 2} \sum_{r, s = 0}^{\ell - 1} \chi^j (\gamma^{s - r}) = (q^n - 1)\ell.$$

Hence

$$M(k, m) - \frac{q^n \ell 2m}{(q^n - 1)^m} \leq mq^{n/2} \ell m.$$

Using (8) and (9) we see that

$$N^*(k, m) \geq \frac{q^n \ell 2m}{(q^n - 1)^m} - (m + n)q^{n/2}.$$

Since

$$\ell \geq \frac{k}{2} \geq \frac{q^n - 1}{2(q^3 - 1)} \quad \text{and} \quad \frac{n}{2} > 3m,$$

we have

$$N^*(k, m) \geq \frac{q^n}{2m(q^3 - 1)^m} - (m + n)q^{n/2} \geq q^{n - 3m}2^{-m} - (m + n)q^{n/2} = \left( q^{n/2 - 3m} - (m + n) \right)q^{n/2} \geq \left( 2^{n/2 - 4m} - (m + n) \right)q^{n/2}.$$

Since $m < \beta n$, we see that for any $q$ we have $N^*(k, m) > 0$, provided that $n$ is large enough. \[ \Box \]

For example, we see from Theorem 4 that Conjecture 1 fails for, say,

$$\frac{n}{\log n} \cdot \frac{q^n - 1}{q^3 - 1} \geq k \geq \frac{q^n - 1}{q^3 - 1},$$

provided that $n$ is large enough.

Furthermore, it is clear that if we also have $q \to \infty$, then Theorem 4 holds with any $\alpha < 1/6$. 

Copyright © by SIAM. Unauthorized reproduction of this article is prohibited.
Acknowledgment. The author would like to thank Arne Winterhof for careful reading of the manuscript, pointing out a number of imprecisions and valuable suggestions.

REFERENCES


