An Estimate of Incomplete Mixed Character Sums [1] [2]

Mei-Chu Chang[3]

— Dedicated to Endre Szemerédi for his 70th birthday. —

生 日 快 樂！[4]

In this note we consider incomplete mixed character sums over a finite field $\mathbb{F}_{p^n}$ of the form $\sum_{x\in B_H}\psi\big(f(x)\big)\chi(x)$, where ψ is an additive character, $f(x)\in\mathbb{F}_{p^n}$ a polynomial, χ a non-trivial multiplicative character and B_H a 'box' of the form $B_H=\{\sum_{j=1}^n x_j\omega_j : x_j\in[1,H]\}$. (Here $\{\omega_i\}_{i=1}^n$ is an arbitrary basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$.)

If $f(x)=0$ and $n=1$, Burgess' well-known theorem provides a non-trivial estimate under the assumption $H>p^{1/4+\varepsilon}$. A generalization to arbitrary finite fields was obtained in [C1], [C2] and very recently [K], eventually providing a statement of the same strength as Burgess, in $\mathbb{F}_{p^n}$.

If $n=1$ and $f(x)$ is linear, [FI] proved a non-trivial bound assuming $H>p^{1/4+\varepsilon}$. For a general polynomial $f(x)$ the only available result are that of P. Enflo [E] and a comment made by Heath-Brown [H] in the review of [E]. Heath-brown's estimate (for $n=1$) assumes again that $H>p^{1/4+\varepsilon}$ and comes with a saving of the form $p^{-c(\varepsilon)/2^d}$, where d is the degree of $f(x)$.

Our result below treats the situation of a field $\mathbb{F}_{p^n}$ (relying on Konyagin's bound for the multiplicative energy of a box B_H as described above) and a polynomial $f(x)$ of arbitrary degree d, assuming $H>p^{1/4+\varepsilon}$. We obtain a saving over the trivial bound of the form $p^{-c(n,\varepsilon)/(d+1)^2}$, so that, interestingly, even for $n=1$ the result seems new.

Notation and Convention.

1. $e(\theta)=e^{2\pi i\theta}$, $e_p(\theta)=e(\frac{\theta}{p})$
2. When there is no ambiguity, $p^{\,\varepsilon}=[p^{\,\varepsilon}]\in\mathbb{Z}$.

[1]2000 *Mathematics Subject Classification.*Primary 11L40, 11L26; Secondary 11A07, 11B75.
[2]*Key words.* character sums, quadratic residues, Burgess
[3]Research partially financed by the National Science Foundation.
[4]Happy Birthday!

3. Multiplicative energy

$$E(A,B) = \Big|\Big\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1b_1 = a_2b_2\Big\}\Big|.$$

Let $\omega_1,\dots,\omega_n$ be an arbitrary basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. Then for any $x \in \mathbb{F}_{p^n}$, there is a unique representation of x in terms of the basis.

$$x = x_1\omega_1 + \cdots + x_n\omega_n.$$

A *box* $B_H \subset \mathbb{F}_{p^n}$ *of size* H is a set such that for each j, the coefficients x_j form an interval.

$$B_H = \Big\{\sum_{j=1}^{n} x_j\omega_j : x_j \in [1,H], \quad \forall j\Big\}. \tag{1}$$

Theorem. *Let χ (respectively, ψ) be a non-principal multiplicative (resp. additive) character of $\mathbb{F}_{p^n}$. For a basis $\omega_1,\omega_2,\dots,\omega_n$ of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, let B_H be a box as defined in (1) by the basis with*

$$H > p^{\frac{1}{4}+\kappa} \text{ for some } \kappa > 0. \tag{2}$$

Then for a polynomial $f \in \mathbb{F}_{p^n}$ of degree d, we have

$$\Big|\sum_{x\in B_H} \psi\big(f(x)\big)\chi(x)\Big| < c(n,\kappa)(d+1)^2 p^{-\delta}|B|,$$

where

$$\delta = \frac{\kappa^2 n}{4(1+2\kappa)(2n+(d+1)^2)}$$

and $c(n,\kappa)$ is a constant depending on n and κ.

Sketch of Proof.

As in [C1], [C2] and [K], we use Burgess' method [Bu1].

Let $\varepsilon > 0$ be specified later (see (16)) and let $B_{p^{-2\varepsilon}H}$ be a box of size $p^{-2\varepsilon}H$ as defined in (1). For $y \in B_{p^{-2\varepsilon}H}$ and $0 < t < p^{\varepsilon}$, since $yt \in B_{p^{-\varepsilon}H}$, we have

$$\Big|\sum_{x\in B_H} \psi\big(f(x)\big)\chi(x) - \sum_{x\in B_H} \psi\big(f(x+yt)\big)\chi(x+yt)\Big|$$
$$\le \Big|B \setminus (B+yt)\Big| + \Big|(B+yt)\setminus B\Big| < 2np^{-\varepsilon}H^n.$$

Hence

$$\Big|\sum_{x\in B_H}\psi\big(f(x)\big)\chi(x)\Big|$$
$$\leq\frac{1}{p^{\,\varepsilon}|B_{p^{-2\varepsilon}H}|}\Big|\sum_{\substack{x\in B_H,\,y\in B_{p^{-2\varepsilon}H}\\ 0<t<p^{\varepsilon}}}\psi\big(f(x+yt)\big)\chi(x+yt)\Big|+O(p^{-\varepsilon}H^n). \tag{3}$$

An additive character is of this form

$$\psi(z)=e_p(Tr\ \xi z),\quad \text{for some } \xi\in\mathbb{F}_{p^n}.$$

Expanding

$$f(x+yt)=a_d(x,y)t^d+a_{d-1}(x,y)t^{d-1}+\cdots+a_0(x,y),$$

and we write

$$\psi\big(f(x+yt)\big)=e\bigg(\sum_{j=0}^{d}\frac{Tr\ \xi a_j(x,y)}{p}\ t^j\bigg). \tag{4}$$

Fix $\varepsilon_1>0$ (to be specified later) and partition $[0,1]^{d+1}$ in boxes Q_α of size $p^{-\varepsilon_1}$. There are $p^{\,\varepsilon_1(d+1)}$ boxes. Partition $B_H\times B_{p^{-2\varepsilon}H}$ according to the boxes Q_α.

$$B_H\times B_{p^{-2\varepsilon}H}=\bigcup_\alpha\Omega_\alpha,$$

where

$$\Omega_\alpha=\bigg\{(x,y)\in B_H\times B_{p^{-2\varepsilon}H}:\bigg(\frac{Tr\ \xi a_j(x,y)}{p}\bigg)_{1\leq j\leq d+1}\in Q_\alpha\ (\mathrm{mod}\ 1)\bigg\}.$$

Hence for $\theta_\alpha=(\theta_{\alpha,1},\dots,\theta_{\alpha,d+1})\in Q_\alpha$ and $(x,y)\in\Omega_\alpha$, we have

$$\bigg|\frac{Tr\ \xi a_j(x,y)}{p}-\theta_{\alpha,j}\bigg|<p^{-\varepsilon_1},\ \text{for } j=1,\dots,d+1. \tag{5}$$

Since $t<p^{\,\varepsilon}$, (4) and (5) imply that for $(x,y)\in\Omega_\alpha$,

$$\begin{aligned}&\bigg|\psi\big(f(x+yt)\big)-e\Big(\sum_{j=0}^{d}\theta_{\alpha,j}\ t^j\Big)\bigg|\\ &\leq 2\pi\sum_j\bigg|\frac{Tr\ \xi a_j(x,y)}{p}-\theta_{\alpha,j}\bigg|\ t^j\\ &<2\pi(d+1)p^{d\varepsilon-\varepsilon_1}\lesssim p^{-\varepsilon},\end{aligned} \tag{6}$$

for

$$\varepsilon_1 = (d+1)\varepsilon. \tag{7}$$

Therefore, the bound in (3) is bounded by

$$\frac{1}{p^{\,\varepsilon}|B_{p^{-2\varepsilon}H}|}\sum_{\alpha}\sum_{(x,y)\in\Omega_\alpha}\Bigg|\sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d}\theta_{\alpha,j}\ t^j\Big)\ \chi(x+yt)\Bigg| + O(p^{-\varepsilon}H^n). \tag{8}$$

For $z\in\mathbb{F}_{p^n}$, denote

$$\mu_\alpha(z) = \Big|\Big\{(x,y)\in\Omega_\alpha : \frac{x}{y} = z\Big\}\Big|. \tag{9}$$

The sum in the first term of (8) equals

$$\sum_{\alpha}\sum_{z\in\mathbb{F}_{p^n}}\mu_\alpha(z)\Bigg|\sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d}\theta_{\alpha,j}\ t^j\Big)\ \chi(z+t)\Bigg|. \tag{10}$$

Take $r\in\mathbb{Z}$ specified later. Hölder's inequality bounds (10) by

$$\underbrace{\Big(\sum_{\alpha}\sum_{z\in\mathbb{F}_{p^n}}\ \mu_\alpha(z)^{\frac{2r}{2r-1}}\Big)^{1-\frac{1}{2r}}}_{(A)}\ \underbrace{\Bigg(\sum_{\alpha}\sum_{z\in\mathbb{F}_{p^n}}\Bigg|\sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d}\theta_{\alpha,j}\ t^j\Big)\ \chi(z+t)\Bigg|^{2r}\Bigg)^{\frac{1}{2r}}}_{(B)}. \tag{11}$$

Hölder's inequality also gives

$$\begin{aligned}(A) &\le \Big(\sum_{\alpha,z}\ \mu_\alpha(z)\Big)^{1-\frac{1}{r}}\ \Big(\sum_{\alpha,z}\ \mu_\alpha(z)^2\Big)^{\frac{1}{2r}}\\ &= (\sum_{\alpha}|\ \Omega_\alpha|)^{1-\frac{1}{r}}E(B_H, B_{p^{-2\varepsilon}H})^{\frac{1}{2r}} \qquad (12)\\ &\le c(n)\big(p^{-2\varepsilon}H^2\big)^{n(1-\frac{1}{r})}\Big(p^{-2n\varepsilon}H^{2n}\Big)^{\frac{1}{2r}}\ \log p\ .\end{aligned}$$

Here the equality follows from the definitions of $\mu_\alpha(z)$ and the multiplicative energy. For the last inequality, we use Konyagin's bound on multiplicative energy [K] and that

$$E(B_H, B_{p^{-2\varepsilon}H}) \le E\big(B_H, B_H\big)^{\frac{1}{2}}\ E\big(B_{p^{-2\varepsilon}H}, B_{p^{-2\varepsilon}H}\big)^{\frac{1}{2}}.$$

$\big($This is by Cauchy-Schwarz. (See [TV] Corollary 2.10.)$\big)$

To bound (B), we write

$$(B)^{2r} = \sum_{\alpha} B_\alpha$$

with

$$B_\alpha = \sum_z \Big| \sum_{t=1}^{p^{\,\varepsilon}} e\big(\sum_{j=0}^{d} \theta_{\alpha,j}\; t^j \big)\; \chi(z+t) \Big|^{2r}.$$

For fixed α, we expand $\Big| \sum_{t=1}^{p^{\,\varepsilon}} e\big(\sum_{j=0}^{d} \theta_{\alpha,j}\; t^j \big)\; \chi(z+t) \Big|^{2r}$ and obtain

$$\begin{aligned} &\Big| \sum_{t=1}^{p^{\,\varepsilon}} e\Big(\sum_{j=0}^{d} \theta_{\alpha,j}\; t^j \Big)\; \chi(z+t) \Big|^{2r} \\ = &\sum_{t_1,\ldots,\, t_{2r}} c_\alpha(t_1, \ldots, t_{2r}) \chi\Big(\frac{(z+t_1)\cdots(z+t_r)}{(z+t_{r+1})\cdots(z+t_{2r})} \Big) \end{aligned} \tag{13}$$

with $|c_\alpha(t_1, \ldots, t_{2r})| = 1$. This gives

$$\begin{aligned} (B)^{2r} &\leq (2r)^{2r} p^{\,\varepsilon_1(d+1)} \sum_{t_1,\ldots,\, t_{2r} < p^{\varepsilon}} \Big| \sum_z \chi\Big(\frac{(z+t_1)\cdots(z+t_r)}{(z+t_{r+1})\cdots(z+t_{2r})} \Big) \Big| \\ &\leq (2r)^{2r} p^{\,\varepsilon_1(d+1)} \Big[p^n p^{r\varepsilon} + p^{\frac{n}{2}} p^{2r\varepsilon} \Big] \end{aligned}$$

(The last inequality is given by Weil's estimate.)

Therefore,

$$(B) < crp^{\,\frac{\varepsilon_1(d+1)}{2r}} \Big[p^{\frac{n}{2r}+\frac{\varepsilon}{2}} + p^{\frac{n}{4r}+\varepsilon} \Big]. \tag{14}$$

Putting (10)-(12) and (14) together, we have the first term of (8) bounded by

$$\begin{aligned} &\frac{c(n) r \log p}{p^{\,\varepsilon} (p^{-2\varepsilon} H)^n} \big(p^{-2\varepsilon} H^2 \big)^{n(1-\frac{1}{r})} \Big(p^{-2n\varepsilon} H^{2n} \Big)^{\frac{1}{2r}} p^{\,\frac{\varepsilon_1(d+1)}{2r}} \Big[p^{\frac{n}{2r}+\frac{\varepsilon}{2}} + p^{\frac{n}{4r}+\varepsilon} \Big] \\ \leq & c(n) r\ \log p\ \ H^{n-\frac{n}{r}} p^{\frac{\varepsilon_1(d+1)}{2r}+\frac{\varepsilon n}{r}} \Big[p^{\frac{n}{2r}-\frac{\varepsilon}{2}} + p^{\frac{n}{4r}} \Big] \\ \leq & c(n) r\ H^n p^{\frac{\varepsilon}{2r}\big((d+1)^2+2n\big)} \Big[\Big(\frac{p^{\frac{1}{2}}}{H} \Big)^{\frac{n}{r}} p^{-\frac{\varepsilon}{2}} + \Big(\frac{p^{\frac{1}{4}}}{H} \Big)^{\frac{n}{r}} \Big] \\ < & c(n) r\ H^n p^{\frac{\varepsilon}{2r}\big((d+1)^2+2n\big)} \Big[p^{\frac{n}{4r}-\frac{\varepsilon}{2}} + p^{-\kappa\frac{n}{r}} \Big]. \end{aligned} \tag{15}$$

(The last inequality is by our assumption (2).)

Take

$$\varepsilon = \kappa \ \frac{n}{(d+1)^2 + 2n} \tag{16}$$

and

$$r = \left\lceil (2\kappa+1)\frac{n}{\varepsilon} \right\rceil = \left\lceil \Big((d+1)^2 + 2n\Big)\Big(2 + \frac{1}{\kappa}\Big) \right\rceil. \tag{17}$$

Substituting (16) in the second factor of (15), we obtain $p^{\frac{\kappa n}{2r}}$. Our choice of r implies that $r > (2\kappa+1)\frac{n}{\varepsilon}$ and hence $\frac{\kappa n}{2r} + \frac{n}{4r} < \frac{\varepsilon}{4}$. Therefore, (15) is bounded by

$$c(n,\kappa)(d+1)^2 H^n (p^{-\frac{\varepsilon}{4}} + p^{-\kappa\frac{n}{2r}}) < c(n,\kappa)(d+1)^2 H^n p^{-\frac{\kappa^2 n}{4(1+2\kappa)((d+1)^2+2n)}}.$$

$\Big($The inequality is because $r < 2\big((d+1)^2 + 2n\big)\big(2 + \frac{1}{\kappa}\big)$ by (17).$\Big)$

Remark. One may estimate the quantity

$$\sum_{t_1,\ldots,\, t_{2r}} \Big| \sum_{\alpha} c_\alpha(t_1, \ldots, t_{2r}) \Big|,$$

which essentially equals to

$$\int_{\Pi^{d+1}} \Big| \sum_{t=1}^{p^{\varepsilon}} e\Big(\sum_{j=0}^{d} \theta_j\, t^j \Big) \Big|^{2r} d\theta_0 \cdots d\theta_d$$

and may be estimated using the classical Vinogradov's mean value theorem. This will lead to some further saving of δ that may be significant for specific values of κ and d. In the context of our theorem where we focus on small κ and large d, the improvement turns out to be without interest.

Acknowledgement. The author would like to thank referee for many helpful comments. The author would also like to thank Lih-Chung Wang for technical support.

References

[Bu1] D.A. Burgess, *On character sums and primitive roots*, Proc LMS (3), 12, (1962), 179-192.

[BC] J. Bourgain, M.-C. Chang, *On a multilinear character sum of Burgess*, Comptes rendus - Mathematique, to appear.

[C1] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*, Duke Math. J. 145 (2008), No. 3, 409–442.

[C2] ______, *Burgess inequality in F_{p^2}*, Geom. Funct. Anal, to appear.

[C3] ______, *Character Sums in Finite Fields*, AMS Contemporary Mathematics Series, to appear.

[E] P. Enflo, *Some problems in the interface between number theory, harmonic analysis and geometry of Euclidean space*, First International Conference in Abstract Algebra, Quaestiones Math. 18 (1995), no. 1-3, 309-323.

[FI] J. Friedlander, H. Iwaniec, *Estimates for character sums*, Proc. Amer. Math. Soc. 119, No 2, (1993), 265-372.

[H] D.R. Heath-Brown, *MR1340486 (96h:11079).*

[K] S.V. Konyagin, *Estimates of character sums in finite fields*, Matematicheskie Zametki, to appear, (in Russian).

[TV] T. Tao, V. Vu *Additive Combinatorics*, Cambridge University Press, (2006).

Department Of Mathematics, University Of California, Riverside, CA 92521

E-mail address: `mcc@math.ucr.edu`