# Evaluating Binomial Character Sums Modulo Powers of Two 

Vincent PIGNO, Chris PINNER*, Joe SHEPPARD<br>Department of Mathematics, Kansas State University, Manhattan, KS 66506, USA


#### Abstract

We show that for any mod $2^{m}$ characters, $\chi_{1}, \chi_{2}$, the complete exponential sum, $\sum_{x=1}^{2^{m}} \chi_{1}(x) \chi_{2}\left(A x^{k}+B\right)$ has a simple explicit evaluation.


Keywords character sums
MR(2010) Subject Classification 11L05; 11L03; 11L10

## 1. Introduction

Suppose that $\chi_{1}$ and $\chi_{2}$ are $\bmod 2^{m}$ multiplicative characters with $\chi_{2}$ primitive mod $2^{m}$, $m \geq 3$. We are interested here in evaluating the complete character sum

$$
S=\sum_{x=1}^{2^{m}} \chi_{1}(x) \chi_{2}\left(A x^{k}+B\right)
$$

Writing $\chi\left(A x^{K}+B x^{L}\right)=\chi^{L}(x) \chi\left(A x^{K-L}+B\right)$ these sums of course include the binomial character sums. Cases where one can explicitly evaluate an exponential or character sum are unusual and therefore worth investigating.

In [8] we considered the corresponding result for $\bmod p^{m}$ characters with $p \geq 3$ and $m$ sufficiently large, using reduction techniques of Cochrane [2] and Cochrane \& Zheng [3,4]. Though their results are stated for odd primes, the approach can often be adapted for $p=2$ as we showed for twisted monomial exponential sums in [7]. When $k=1$ and $A=-1, B=1$, the $\bmod p^{m}$ sum is the classical Jacobi sum (though uninterestingly zero if $p=2$ ). See [1] or [5] for an extensive treatment of mod $p$ Jacobi sums and their generalizations over $\mathbb{F}_{p^{m}}$. In [6] we treated the $k=1$ case for general $A, B$, including when $p=2$, along with generalizations of the multivariable Jacobi sums considered in [9].

Plainly $S=0$ if $A$ and $B$ are not of opposite parity (otherwise $x$ or $A x^{k}+B$ will be even and the individual terms will all be zero). We assume here that $A$ is even and $B$ is odd and write

$$
A=2^{n} A_{1}, n>0, \quad k=2^{t} k_{1}, \quad 2 \nmid A_{1} k_{1} B .
$$

[^0]If $B$ is even and $A$ odd, we can use $x \mapsto x^{-1}$ to write $S$ in the form

$$
S=\sum_{x=1}^{2^{m}} \bar{\chi}_{1} \bar{\chi}_{2}^{k}(x) \chi_{2}\left(B x^{k}+A\right)
$$

Since $\mathbb{Z}_{2^{m}}^{*}=\langle-1,5\rangle$, the characters $\chi_{1}, \chi_{2}$ are completely determined by their values on -1 and 5 . Since 5 has order $2^{m-2} \bmod 2^{m}$, we can define integers $c_{1}, c_{2}$ with

$$
\chi_{i}(5)=e_{2^{m-2}}\left(c_{i}\right), \quad 1 \leq c_{i} \leq 2^{m-2},
$$

where $e_{n}(x):=e^{2 \pi i x / n}$. Since $\chi_{2}$ is primitive, we have $2 \nmid c_{2}$. We define the odd integers $R_{i}$, $i \geq 2$, by

$$
\begin{equation*}
5^{2^{i-2}}=1+R_{i} 2^{i} . \tag{1}
\end{equation*}
$$

Defining

$$
N:= \begin{cases}\left\lceil\frac{1}{2}(m-n)\right\rceil, & \text { if } m-n>2 t+4 \\ t+2, & \text { if } t+2 \leq m-n \leq 2 t+4\end{cases}
$$

and

$$
\begin{equation*}
C(x):=c_{1}\left(A x^{k}+B\right)+c_{2} A k x^{k} R_{N} R_{N+n}^{-1} \tag{2}
\end{equation*}
$$

(here and throughout the paper $y^{-1}$ denotes the inverse of $y \bmod 2^{m}$ ) it transpires that the sum $S$ will be zero unless there is a solution $x_{0}$ to the characteristic equation

$$
\begin{equation*}
C\left(x_{0}\right) \equiv 0 \bmod 2^{\left\lfloor\frac{1}{2}(m+n)\right\rfloor+t}, \tag{3}
\end{equation*}
$$

with $2 \nmid x_{0}\left(A x_{0}^{k}+B\right)$, when $m-n>2 t+4$, and a solution to $C(1)$ or $C(-1) \equiv 0 \bmod 2^{m-2}$ when $t+2 \leq m-n \leq 2 t+4$.

Theorem 1.1 Suppose that $m-n \geq t+2$. The sum $S=0$ unless $c_{1}=2^{n+t} c_{3}$, with $2 \nmid c_{3}$, and $\chi_{1}(-1)=1$ when $k$ is even, and the characteristic equation (3) has an odd solution $x_{0}$ when $m-n>2 t+4$. Assuming these conditions do hold.

When $m-n>2 t+4$,

$$
S=2^{\frac{1}{2}(m+n)+t+\min \{1, t\}} \chi_{1}\left(x_{0}\right) \chi_{2}\left(A x_{0}^{k}+B\right) \begin{cases}1, & \text { if } m-n \text { is even }, \\ \omega^{h}\left(\frac{2}{h}\right), & \text { if } m-n \text { is odd },\end{cases}
$$

where $\left(\frac{2}{x}\right)$ is the Jacobi symbol, $\omega=e^{\pi i / 4}, C\left(x_{0}\right)=\lambda 2^{\left\lfloor\frac{1}{2}(m+n)\right\rfloor+t}$ for some integer $\lambda$ and $h:=2 \lambda+\left(k_{1}-1\right)+\left(2^{n}-1\right) c_{3}$.

When $t+3<m-n \leq 2 t+4$,

$$
S= \begin{cases}2^{m-1} \chi_{2}(A+B), & \text { if } k \text { is even and } C(1) \equiv 0 \bmod 2^{m-2} \\ 2^{m-2} \chi_{2}(A+B), & \text { if } k \text { is odd and } C(1) \equiv 0 \bmod 2^{m-2} \\ 2^{m-2} \chi_{1}(-1) \chi_{2}(-A+B), & \text { if } k \text { is odd and } C(-1) \equiv 0 \bmod 2^{m-2}, \\ 0, & \text { otherwise. }\end{cases}
$$

When $m-n=t+3$,

$$
S= \begin{cases}2^{m-1} \chi_{2}(A+B), & \text { if } k \text { is even and } \chi_{1}(5)= \pm 1, \chi_{1}(-1)=1, \\ 2^{m-2}\left(\chi_{2}(A+B)+\chi_{1}(-1) \chi_{2}(-A+B)\right), & \text { if } k \text { is odd and } \chi_{1}(5)= \pm 1, \\ 0, & \text { otherwise } .\end{cases}
$$

When $m-n=t+2$,

$$
S= \begin{cases}2^{m-1} \chi_{2}(A+B), & \text { if } k \text { is even and } \chi_{1}=\chi_{0} \text { or } k \text { is odd and } \chi_{1}=\chi_{4} \\ 0, & \text { otherwise },\end{cases}
$$

where $\chi_{0}$ is the principal character $\bmod 2^{m}$ and $\chi_{4}$ is the $\bmod 2^{m}$ character induced by the non-trivial character $\bmod 4$ (i.e., $\chi_{4}(x)= \pm 1$ as $x \equiv \pm 1 \bmod 4$, respectively).

Note that the restriction $m-n \geq t+2$ is quite natural; for $m-n<t+2$ the odd $x$ will make $A x^{k}+B \equiv A+B \bmod 2^{m}$ and $S=\chi_{2}(A+B) \sum_{x=1}^{2^{m}} \chi_{1}(x)=2^{m-1} \chi_{2}(A+B)$ if $\chi_{1}=\chi_{0}$ and zero otherwise.

Our original assumption that $\chi_{2}$ is primitive is also reasonable; if $\chi_{1}$ and $\chi_{2}$ are both imprimitive, then one should reduce the modulus, while if $\chi_{1}$ is primitive and $\chi_{2}$ imprimitive, then $S=0$ (if $\chi_{1}$ is primitive then $u=1+2^{m-1}$ must have $\chi_{1}(u)=-1$, since $x+2^{m-1} \equiv u x$ $\bmod 2^{m}$ for any odd $x$, and $x \mapsto x u$ gives $S=\chi_{1}(u) S$ when $\chi_{2}$ is imprimitive).

## 2. Proof

## Initial decomposition

Observing that $\pm 5^{\gamma}, \gamma=1, \ldots, 2^{m-2}$, gives a reduced residue system $\bmod 2^{m}$ and writing

$$
S(A):=\sum_{\gamma=1}^{2^{m-2}} \chi_{1}\left(5^{\gamma}\right) \chi_{2}\left(A 5^{\gamma k}+B\right)
$$

if $k$ is even we have

$$
S=\left(1+\chi_{1}(-1)\right) S(A)= \begin{cases}0, & \text { if } \chi_{1}(-1)=-1  \tag{4}\\ 2 S(A), & \text { if } \chi_{1}(-1)=1,\end{cases}
$$

and if $k$ is odd

$$
\begin{equation*}
S=S(A)+\chi_{1}(-1) S(-A) \tag{5}
\end{equation*}
$$

Large $m$ values: $m>n+2 t+4$
If $I_{1}$ is an interval of length $2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}$, then plainly

$$
\gamma=u 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}+v, \quad v \in I_{1}, \quad u \in I_{2}:=\left[1,2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t}\right]
$$

runs through a complete set of residues mod $2^{m-2}$. Hence, writing $h(x):=A x^{k}+B$ and noting that $2 \nmid h\left(5^{v}\right)$,

$$
\begin{aligned}
S(A) & =\sum_{v \in I_{1}} \chi_{1}\left(5^{v}\right) \sum_{u \in I_{2}} \chi_{1}\left(5^{u 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}}\right) \chi_{2}\left(A 5^{v k} 5^{k u 2^{\left.\frac{m-n}{2}\right\rceil-t-2}}+B\right) \\
& =\sum_{v \in I_{1}} \chi_{1}\left(5^{v}\right) \chi_{2}\left(h\left(5^{v}\right)\right) \sum_{u \in I_{2}} \chi_{1}\left(5^{u 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}}\right) \chi_{2}(W)
\end{aligned}
$$

where

$$
W=h\left(5^{v}\right)^{-1} A 5^{v k}\left(5^{k u 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}}-1\right)+1 .
$$

Since $n+2\left\lceil\frac{m-n}{2}\right\rceil \geq m$ and $2\left\lceil\frac{m+n}{2}\right\rceil \geq m$, we have

$$
W=A_{1} 5^{v k} h\left(5^{v}\right)^{-1} 2^{n}\left(\left(1+R_{\left\lceil\frac{m-n}{2}\right\rceil} 2^{\left\lceil\frac{m-n}{2}\right\rceil}\right)^{u k_{1}}-1\right)+1
$$

$$
\begin{aligned}
& \equiv 1+A_{1} 5^{v k} h\left(5^{v}\right)^{-1} u k_{1} R_{\left\lceil\frac{m-n}{2}\right\rceil} 2^{\left\lceil\frac{m+n}{2}\right\rceil} \bmod 2^{m} \\
& \equiv\left(1+R_{\left.\left\lceil\frac{m+n}{2}\right\rceil{ }^{\left\lceil\frac{m+n}{2}\right\rceil}\right)^{A_{1} 5^{v k} h\left(5^{v}\right)^{-1} u k_{1} R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1} \bmod 2^{m}}}^{=5^{A_{1} 5^{v k} h\left(5^{v}\right)^{-1} u k_{1} R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1} 2^{\left.2 \frac{m+n}{2}\right\rceil-2}}} \begin{array}{c} 
\\
=5^{A 5^{v k} h\left(5^{v}\right)^{-1} u k R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1} 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}} .
\end{array} .\right.
\end{aligned}
$$

So we can write

$$
\sum_{u \in I_{2}} \chi_{1}\left(5^{u 2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}}\right) \chi_{2}(W)=\sum_{u \in I_{2}} e_{2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t}}\left(u\left(c_{1}+c_{2} A 5^{v k} h\left(5^{v}\right)^{-1} k R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1}\right)\right)
$$

which equals $2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t}$ for the $v$ with

$$
\begin{equation*}
c_{1} h\left(5^{v}\right)+c_{2} A 5^{v k} k R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1} \equiv 0 \bmod 2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t} \tag{6}
\end{equation*}
$$

and zero otherwise. Since $m \geq n+2$, equation (6) has no solution (and hence $S=0$ ) unless $c_{1}=2^{n+t} c_{3}$ with $2 \nmid c_{3}$, in which case (6) becomes

$$
\begin{equation*}
\left(c_{3} A+c_{2} A_{1} k_{1} R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1}\right) 5^{v k} \equiv-c_{3} B \bmod 2^{\left\lfloor\frac{m-n}{2}\right\rfloor} . \tag{7}
\end{equation*}
$$

If no $v$ satisfies (6), then plainly $S=0$. So assume that (6) has a solution $v=v_{0}$ and take $I_{1}=\left[v_{0}, v_{0}+2^{\left\lceil\frac{m-n}{2}\right\rceil-t-2}\right)$. Now any other $v$ solving (7) must have

$$
5^{v k} \equiv 5^{v_{0} k} \bmod 2^{\left\lfloor\frac{m-n}{2}\right\rfloor} \Rightarrow v k \equiv v_{0} k \bmod 2^{\left\lfloor\frac{m-n}{2}\right\rfloor-2} \Rightarrow v \equiv v_{0} \bmod 2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2} .
$$

So if $m-n$ is even, $I_{1}$ contains only the solution $v_{0}$ and

$$
\begin{equation*}
S(A)=2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t} \chi_{1}\left(5^{v_{0}}\right) \chi_{2}\left(A 5^{v_{0} k}+B\right) . \tag{8}
\end{equation*}
$$

Observe that a solution $x_{0}=5^{v_{0}}$ or $x_{0}=-5^{v_{0}}$ of (3) corresponds to a solution $v_{0}$ to (6) when $k$ is even and a solution $v_{0}$ to (6) for $A$ or $-A$ respectively (both cannot have solutions) if $k$ is odd. The evaluation for $S$ follows at once from (8) and (4) or (5). When $m-n$ is odd, $I_{1}$ contains two solutions $v_{0}$ and $v_{0}+2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2}$ and

$$
\begin{aligned}
S(A) & =2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t} \chi_{1}\left(5^{v_{0}}\right)\left(\chi_{2}\left(h\left(5^{v_{0}}\right)\right)+\chi_{1}\left(5^{\left.2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2}\right)} \chi_{2}\left(A 5^{v_{0} k} 5^{k 2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2}}+B\right)\right)\right. \\
& =2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t} \chi_{1}\left(5^{v_{0}}\right) \chi_{2}\left(h\left(5^{v_{0}}\right)\right)\left(1+\chi_{1}\left(5^{2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2}}\right) \chi_{2}(\xi)\right)
\end{aligned}
$$

where, since $3\left\lfloor\frac{m-n}{2}\right\rfloor+n \geq m$ for $m \geq n+3$,

$$
\begin{aligned}
\xi & =A 5^{v_{0} k}\left(5^{k_{1} 2^{\left\lfloor\frac{m-n}{2}\right\rfloor-2}}-1\right) h\left(5^{v_{0}}\right)^{-1}+1 \\
& =A 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1}\left(\left(1+R_{\left\lfloor\frac{m-n}{2}\right\rfloor} 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}\right)^{k_{1}}-1\right)+1 \\
& \equiv A 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1}\left(k_{1} R_{\left\lfloor\frac{m-n}{2}\right\rfloor} 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}+\binom{k_{1}}{2} R_{\left\lfloor\frac{m-n}{2}\right\rfloor}^{2} 2^{m-n-1}\right)+1 \bmod 2^{m} \\
& \equiv\left(A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}+\frac{1}{2}\left(k_{1}-1\right) 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}\right) R_{\left\lfloor\frac{m+n}{2}\right\rfloor} 2^{\left\lfloor\frac{m+n}{2}\right\rfloor}+1 \bmod 2^{m} \\
& \left.\equiv\left(1+R_{\left\lfloor\frac{m+n}{2}\right\rfloor}\right\rfloor^{\left\lfloor\frac{m+n}{2}\right\rfloor}\right)^{A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}+\frac{1}{2}\left(k_{1}-1\right) 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}} \bmod 2^{m} \\
& =5^{\left(A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}+\frac{1}{2}\left(k_{1}-1\right) 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}\right) 2^{\left\lfloor\frac{m+n}{2}\right\rfloor-2}} .
\end{aligned}
$$

Hence, setting

$$
c_{3}+c_{2} A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1}=\lambda 2^{\left\lfloor\frac{m-n}{2}\right\rfloor}
$$

(only the parity of $\lambda$ will be used) and recalling that $c_{2}$ is odd, we have

$$
\begin{aligned}
& \chi_{1}\left(5^{2^{\left\lfloor\frac{m-n}{2}\right\rfloor-t-2}}\right) \chi_{2}(\xi)=e_{2^{\left\lceil\frac{m-n}{2}\right\rceil}}\left(c_{3}+c_{2} A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}\right)(-1)^{\frac{1}{2}\left(k_{1}-1\right) c_{2}} \\
& \quad=e_{2^{\left\lceil\frac{m-n}{2}\right\rceil}}\left(c_{2} A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1}\left(R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}-R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1}\right)\right)(-1)^{\frac{1}{2}\left(k_{1}-1\right)+\lambda}
\end{aligned}
$$

Since $1+R_{i+1} 2^{i+1}=\left(1+R_{i} 2^{i}\right)^{2}$, we have $R_{i+1}=R_{i}+2^{i-1} R_{i}^{2} \equiv R_{i}+2^{i-1} \bmod 2^{i+2}$, giving $R_{i} \equiv 3 \bmod 4$ for $i \geq 3$, and

$$
\begin{aligned}
& R_{\left\lfloor\frac{m-n}{2}\right\rfloor} R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1}-R_{\left\lceil\frac{m-n}{2}\right\rceil} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1} \equiv R_{\left\lfloor\frac{m+n}{2}\right\rfloor}^{-1} R_{\left\lceil\frac{m+n}{2}\right\rceil}^{-1}\left(\left(R_{\left\lceil\frac{m-n}{2}\right\rceil}-2^{\left\lceil\frac{m-n}{2}\right\rceil-2}\right) R_{\left\lceil\frac{m+n}{2}\right\rceil}-\right. \\
& \left.R_{\left\lceil\frac{m-n}{2}\right\rceil}\left(R_{\left\lceil\frac{m+n}{2}\right\rceil}-2^{\left\lceil\frac{m-n}{2}\right\rceil+n-2}\right)\right) \bmod 2^{\left\lceil\frac{m-n}{2}\right\rceil} \\
& \equiv\left(1-2^{n}\right) 2^{\left\lceil\frac{m-n}{2}\right\rceil-2} \bmod 2^{\left\lceil\frac{m-n}{2}\right\rceil} .
\end{aligned}
$$

From (6) we have $c_{2} A_{1} 5^{v_{0} k} h\left(5^{v_{0}}\right)^{-1} k_{1} \equiv-c_{3} \bmod 4$ and

$$
S(A)=2^{\left\lfloor\frac{m+n}{2}\right\rfloor+t} \chi_{1}\left(5^{v_{0}}\right) \chi_{2}\left(h\left(5^{v_{0}}\right)\right)\left(1+i^{\left(2^{n}-1\right) c_{3}}(-1)^{\frac{1}{2}\left(k_{1}-1\right)+\lambda}\right) .
$$

The result follows on writing $\frac{1+i^{h}}{\sqrt{2}}=\omega^{h}\left(\frac{2}{h}\right)$.
Small $m$ values: $t+2 \leq m-n \leq 2 t+4$
Since $n+2(t+2) \geq m$, we have

$$
\begin{aligned}
A 5^{\gamma k}+B & =A_{1} 2^{n}\left(1+R_{t+2} 2^{t+2}\right)^{\gamma k_{1}}+B \\
& \equiv(A+B)\left(1+\gamma k_{1} A_{1} R_{t+2}(A+B)^{-1} 2^{t+n+2}\right) \bmod 2^{m} \\
& \equiv(A+B)\left(1+R_{t+n+2} 2^{t+n+2}\right)^{\gamma k_{1} A_{1}(A+B)^{-1} R_{t+2} R_{t+n+2}^{-1} \bmod 2^{m}} \\
& =(A+B) 5^{\gamma A k(A+B)^{-1} R_{t+2} R_{t+n+2}^{-1} .}
\end{aligned}
$$

Hence $\chi_{1}\left(5^{\gamma}\right) \chi_{2}\left(A 5^{\gamma k}+B\right)$ equals

$$
\chi_{2}(A+B) e_{2^{m-2}}\left(\gamma\left(c_{1}(A+B)+c_{2} A k R_{t+2} R_{t+n+2}^{-1}\right)(A+B)^{-1}\right)
$$

and $S(A)=2^{m-2} \chi_{2}(A+B)$ if $C(1) \equiv 0 \bmod 2^{m-2}$ and 0 otherwise. Since $m-n \geq t+2$, the congruence $C(1) \equiv 0 \bmod 2^{m-2}$ implies $c_{1}=2^{t+n} c_{3}$ (with $c_{3}$ odd if $m-n>t+2$ ) and becomes

$$
\begin{equation*}
c_{3}(A+B)+c_{2} A_{1} k_{1} R_{t+2} R_{t+n+2}^{-1} \equiv 0 \bmod 2^{m-n-t-2} . \tag{9}
\end{equation*}
$$

For $m-n=t+2$ or $t+3$ this will automatically hold (for both $A$ and $-A$ when $k$ is odd) and $S=2^{m-1} \chi_{2}(A+B)$ for $k$ even and $\chi_{1}(-1)=1$, and

$$
S=2^{m-2}\left(\chi_{2}(A+B)+\chi_{1}(-1) \chi_{2}(-A+B)\right)
$$

for $k$ odd. Further for $k$ odd and $m-n=2$ we have $-A+B \equiv\left(1+2^{m-1}\right)(A+B) \bmod 2^{m}$ with $\chi_{2}\left(1+2^{m-1}\right)=-1$ and $S=2^{m-2} \chi_{2}(A+B)\left(1-\chi_{1}(-1)\right)=2^{m-1} \chi_{2}(A+B)$ if $\chi_{1}(-1)=-1$ and zero otherwise. Note when $m-n=t+2$, we have $c_{1}=2^{m-2}$ and $\chi_{1}(5)=1$ and when $m-n=t+3$, we have $c_{1}=2^{m-2}$ or $2^{m-3}$ and $\chi_{1}(5)= \pm 1$.

Since $c_{3} B$ is odd, (9) cannot hold for both $A$ and $-A$ for $m-n>t+3$ and at most one of $S(A)$ or $S(-A)$ is non-zero. When $k$ is odd, the congruence condition for $-A$ becomes $C(-1) \equiv 0$ $\bmod 2^{m-2}$.

## References

[1] B. C. BERNDT, R. J. EVANS, K. S. WILLIAMS. Gauss and Jacobi Sums. John Wiley \& Sons, Inc., New York, 1998.
[2] T. COCHRANE. Exponential sums modulo prime powers. Acta Arith., 2002, 101(2): 131-149.
[3] T. COCHRANE, Zhiyong ZHENG. Pure and mixed exponential sums. Acta Arith., 1999, 91(3): 249-278.
[4] T. Cochrane, Zhiyong Zheng. A Survey on Pure and Mixed Exponential Sums Modulo Prime Powers. Number Theory for the Millennium, I (Urbana, IL, 2000), 273-300, A K Peters, Natick, MA, 2002.
[5] R. LIDL, H. NIEDERREITER. Finite Fields, Encyclopedia of Mathematics and Its Applications 20, 2nd Edition, Cambridge University Press, 1997.
[6] M. LONG, V. PIGNO, C. PINNER. Evaluating Prime Power Gauss and Jacobi Sums. arXiv:1410.6179
[7] V. PIGNO, C. PINNER. Twisted monomial Gauss sums modulo prime powers. Funct. Approx. Comment. Math., 2014, 51(2): 285-301.
[8] V. PIGNO, C. PINNER. Binomial Character Sums Modulo Prime Powers. arXiv:1410.6494
[9] Wenpeng ZHANG, Zhefeng XU. On the Dirichlet characters of polynomials in several variables. Acta Arith., 2006, 121(2): 117-124.


[^0]:    Received March 13, 2014; Accepted January 16, 2015
    The first and third authors acknowledge support of K-State's I-Center and Arts \& Sciences Undergraduate Research Scholarships Respectively.

    * Corresponding author

    E-mail address: pignov@math.ksu.edu (Vincent PIGNO); pinner@math.ksu.edu (Chris PINNER); jnsheppa@math.ksu.edu (Joe SHEPPARD)

