On the Connection Between the Maximal Coefficients of the Fourier and Walsh–Hadamard Transforms

Sergey Agievich (agievich@bsu.by)
National Research Center for Applied Problems of Mathematics and Informatics, Belarusian State University, Fr. Skorina av. 4, 220050 Minsk, Belarus

May 21, 2003

Abstract. Let the Fourier and Walsh–Hadamard transforms be applied to the same sequence. We obtain upper bounds for the maximal Fourier coefficient via the maximal Walsh–Hadamard coefficient.

Keywords: Fourier transform, Walsh–Hadamard transform, exponential sums

1. Results

Let $\mathbb{Z}_m$ be the ring of integers modulo m. We identify $\mathbb{Z}_m$ with the set $\{0,1,\dots,m-1\}$ and associate with a vector $\mathbf{x}=(x_0,x_1,\dots,x_{n-1})\in\mathbb{Z}_m^n$, the number

$$x=x_0+mx_1+\ldots+m^{n-1}x_{n-1}\in\{0,1,\dots,m^n-1\}.$$

Let s be a sequence $s_0,s_1,\dots$ over $\mathbb{Z}_m$. To determine some properties of s, the following discrete orthogonal transforms are often applied (see [1, 4, 5] for motivation, details and further references):

The Fourier Transform. Given the elements $s_0,s_1,\dots,s_{r-1}$, calculate the coefficients

$$\mathrm{F}_{s,r}(h)=\sum_{t=0}^{r-1}\chi(s_t)\overline{\omega(ht)},\quad h=0,1,\dots,r-1,$$

where $\chi(a)=\exp(2\pi ia/m)$, $\omega(j)=\exp(2\pi ij/r)$ with $i=\sqrt{-1}$, and the bar indicates complex conjugation.

The Walsh–Hadamard Transform. Given the elements $s_0,s_1,\dots,s_{m^n-1}$, calculate the coefficients

$$\mathrm{WH}_{s,m^n}(\mathbf{b})=\sum_{\mathbf{t}\in\mathbb{Z}_m^n}\chi(s_t)\overline{\chi(\mathbf{b}\cdot\mathbf{t})},\quad \mathbf{b}\in\mathbb{Z}_m^n,$$

where $\mathbf{b}\cdot\mathbf{t}$ is the dot product of two vectors.

For the coefficients given above, the following Parseval's identities hold:

$$\sum_{h=0}^{r-1}|\mathrm{F}_{s,r}(h)|^2=r^2,\quad \sum_{\mathbf{b}\in\mathbb{Z}_m^n}|\mathrm{WH}_{s,m^n}(\mathbf{b})|^2=m^{2n}.$$

Consequently,

$$\max_{0\le h\le r-1}|\mathrm{F}_{s,r}(h)|\ge\sqrt{r},\quad \max_{\mathbf{b}\in\mathbb{Z}_m^n}|\mathrm{WH}_{s,m^n}(\mathbf{b})|\ge m^{n/2}.$$

The problem of constructing sequences s with sufficiently small values of $\max_h |\,\mathrm{F}_{s,r}(h)|$ or $\max_{\mathbf{b}} |\,\mathrm{WH}_{s,m^n}(\mathbf{b})|$, received much attention in some applications. For instance, in cryptography and coding theory bent functions $\mathbb{Z}_m^n \to \mathbb{Z}_m$ are extensively studied (see [2, 6]). If the first m^n elements of s are the values of a bent function on the lexicographically ordered vectors of $\mathbb{Z}_m^n$, then $|\,\mathrm{WH}_{s,n}(\mathbf{b})| = m^{n/2}$ for all $\mathbf{b} \in \mathbb{Z}_m^n$. Another example — m-sequences, i. e. maximal period linear recurrence sequences (see [3]). If m is prime, s is an m-sequence of order n, then s has period $r = m^n - 1$ and $\max_h |\,\mathrm{F}_{s,r}(h)| = \sqrt{r+1}$.

It is natural to look for connections between the coefficients of the transforms above. In particular, it would be interesting to find upper bounds for the Fourier coefficients of bent sequences, on the one hand, and for the Walsh–Hadamard coefficients of m-sequences, on the other hand. In this paper we obtain upper bounds of the first type. Let us state the main result.

Theorem. *For any sequence s over $\mathbb{Z}_m$ and for all positive integers n and r, it holds that*

$$\max_{0\le h\le r-1} |\,\mathrm{F}_{s,r}(h)| \le |m^n - r| + \max_{\mathbf{b}\in\mathbb{Z}_m^n} |\,\mathrm{WH}_{s,m^n}(\mathbf{b})|(S(m))^n, \tag{1}$$

where

$$S(m) = \frac{1}{m}\sum_{a=0}^{m-1} \csc\frac{\pi(2a+1)}{2m}.$$

If $m = 2$ then the term $(S(m))^n$ in (1) can be replaced by

$$\begin{cases} \sqrt{2}\left(\frac{1+\sqrt{3}}{2}\right)^{n-1} & \text{always,} \\ \left(\frac{1+\sqrt{3}}{2}\right)^{n} & \text{if } r = 2^n - 1. \end{cases}$$

It is easy to check that

$$S(3) = \frac{5}{3},\quad S(4) = \sqrt{2+\sqrt{2}},\quad S(5) = \frac{1+4\sqrt{5}}{5},\quad S(6) = \frac{\sqrt{2}+2\sqrt{6}}{3}.$$

Moreover, if $m \ge 3$, then

$$\begin{aligned} S(m) &\le \frac{2}{m}\csc\frac{\pi}{2m} + \frac{1}{m}\int_0^{m-1} \csc\frac{\pi(2x+1)}{2m}dx \\ &\le \frac{4}{3} + \frac{2}{\pi}\int_{\pi/(2m)}^{\pi/2} \csc x dx \\ &= \frac{4}{3} + \frac{2}{\pi}\left(\ln\cos\frac{\pi}{4m} - \ln\sin\frac{\pi}{4m}\right) \\ &< \frac{2}{\pi}\ln m + \frac{4}{3} + \frac{2}{\pi}\ln\frac{4}{3}, \end{aligned}$$

where the inequality $\sin\pi x \ge 3x$, $x \in \left[0, \frac{1}{6}\right]$, is used twice (cf. [3], Lemma 8.80).

In fact we apply the Fourier and Walsh–Hadamard transforms to the sequence $\sigma_0 = \chi(s_0), \sigma_1 = \chi(s_1), \ldots$ of mth complex roots of unity. The estimates of the Theorem can be adapted to the case of an arbitrary complex sequence $\sigma_0, \sigma_1, \ldots$. It is sufficient only to change the term $|m^n - r|$ in (1) to

$$\begin{cases} |\sigma_r| + \ldots + |\sigma_{m^n-1}|, & r < m^n, \\ |\sigma_{m^n}| + \ldots + |\sigma_{r-1}|, & m^n < r. \end{cases}$$

2. Proofs

Start with the auxiliary trigonometric inequality.

Lemma. *For all* $\alpha \in \left[\frac{\pi}{2m}, \pi - \frac{\pi}{2m}\right]$ *and* $y \in \left[-\frac{\pi}{2m}, \frac{\pi}{2m}\right]$, $m = 2, 3, \ldots$, *it holds that*

$$\cos y \cos my \sin^2 \alpha \le \cos^2 y - \cos^2 \alpha. \tag{2}$$

Proof. Rewrite (2) as

$$\sin^2 \alpha (1 - \cos y \cos my) - \sin^2 y \ge 0. \tag{3}$$

It is sufficient to prove the last inequality only for $\alpha = \frac{\pi}{2m}$ and $y \in \left[0, \frac{\pi}{2m}\right]$.

The left-hand side of (3) takes the form

$$\frac{1}{2}(1 - \cos y \cos 2y) - \frac{1}{2}(1 - \cos 2y) = \frac{1}{2}\cos 2y(1 - \cos y)$$

when $m = 2$ and the form

$$\frac{1}{8}(3 - \cos 2y - 2\cos^2 2y) - \frac{1}{2}(1 - \cos 2y) = \frac{1}{8}(1 - \cos 2y)(2\cos 2y - 1)$$

when $m = 3$. In both cases (3) is fulfilled.

For $m \ge 4$, we will prove (3) in two steps: 1) for $y \in \left[0, \frac{3\pi}{8m}\right]$ and 2) for $y \in \left[\frac{3\pi}{8m}, \frac{\pi}{2m}\right]$. Before proceeding, we note that the function $\sin \pi x / x$ decreases on the interval $\left[0, \frac{1}{2}\right]$ and therefore

$$\sin \pi x \ge cx, \quad x \in \left[0, \frac{1}{8}\right], \tag{4}$$

where

$$c = 8 \sin \frac{\pi}{8} = 4\sqrt{2 - \sqrt{2}}, \quad 3 + \frac{1}{17} < c < 3 + \frac{1}{16}.$$

1. If $y \in \left[0, \frac{3\pi}{8m}\right]$, then

$$\begin{aligned} 1 - \cos y \cos my &= \frac{1}{2}(2 - \cos(m-1)y - \cos(m+1)y) \\ &\ge \frac{(m-1)^2 y^2}{4} - \frac{(m-1)^4 y^4}{48} + \frac{(m+1)^2 y^2}{4} - \frac{(m+1)^4 y^4}{48} \\ &= m^2 y^2 \left(\frac{1}{2} - \frac{m^2 y^2}{24}\right) + y^2 \left(\frac{1}{2} - \frac{m^2 y^2}{4} - \frac{y^2}{24}\right) \\ &\ge m^2 y^2 \left(\frac{1}{2} - \frac{3\pi^2}{512}\right). \end{aligned}$$

Now using the estimates $\sin \alpha \ge \frac{c}{2m}$ and $\sin y \le y$, we obtain

$$\sin^2 \alpha (1 - \cos y \cos my) - \sin^2 y \ge \frac{c^2 y^2}{4} \left(\frac{1}{2} - \frac{3\pi^2}{512} - \frac{4}{c^2}\right) \ge 0.$$

2. Let us show that the inequality (3) holds for $y = \alpha - \varepsilon$, $\varepsilon \in [0, \frac{\pi}{8m}]$. Rewrite (3) as

$$\frac{1}{2}(\cos(2\alpha - 2\varepsilon) - \cos 2\alpha) - \sin^2 \alpha \cos(\alpha - \varepsilon) \sin m\varepsilon \geq 0$$

and will prove the stronger inequality

$$g(\varepsilon) = \frac{1}{2}(\cos(2\alpha - 2\varepsilon) - \cos 2\alpha) - \sin^2 \alpha \sin m\varepsilon \geq 0.$$

Since $g(0) = 0$, it is sufficient to show that

$$g'(\varepsilon) = \sin(2\alpha - 2\varepsilon) - m \sin^2 \alpha \cos m\varepsilon \geq 0$$

for all $\varepsilon \in [0, \frac{\pi}{8m}]$. In turn, to prove the last inequality it suffices to show that $g''(\varepsilon) < 0$ and $g'(\varepsilon_m) \geq 0$, $\varepsilon_m = \frac{\pi}{8m}$.

We have

$$\begin{aligned} g''(\varepsilon) &= -2\cos(2\alpha - 2\varepsilon) + m^2 \sin^2 \alpha \sin m\varepsilon \\ &< -2(1 - 2\alpha^2) + m^3 \alpha^2 \varepsilon \\ &= -2 + \frac{\pi^2}{m^2} + \frac{\pi^3}{32} < 0 \end{aligned}$$

and

$$g'(\varepsilon_m) = \sin \frac{3\pi}{4m} - m \sin^2 \frac{\pi}{2m} \cos \frac{\pi}{8}.$$

The inequalities $g'(\varepsilon_{4,5}) \geq 0$ can be verified by direct computation. For $m \geq 6$, using (4), we obtain

$$g'(\varepsilon_m) \geq \frac{3c}{4m} - m \left(\frac{\pi}{2m}\right)^2 \cos \frac{\pi}{8} = \frac{1}{4m} \left(3c - \pi^2 \sqrt{1 - c^2/64}\right) > 0.$$

This completes the proof of the Lemma. □

Turn to the proof of the Theorem. Introduce the exponential sums

$$\pi(\mathbf{b}, h) = \sum_{\tau=0}^{m^n-1} \overline{\chi(\mathbf{b} \cdot \boldsymbol{\tau})} \omega(h\tau), \quad \mathbf{b} \in \mathbb{Z}_m^n, \quad h = 0, \ldots, r-1,$$

and show that

$$|\,\mathrm{F}_{s,r}(h)| \leq |m^n - r| + \frac{1}{m^n} \max_{\mathbf{b} \in \mathbb{Z}_m^n} |\,\mathrm{WH}_{s,m^n}(\mathbf{b})| \sum_{\mathbf{b} \in \mathbb{Z}_m^n} |\pi(\mathbf{b}, h)|. \tag{5}$$

Indeed, for $\mathbf{a} \in \mathbb{Z}_m^n$ it holds that

$$\sum_{\mathbf{b} \in \mathbb{Z}_m^n} \chi(\mathbf{a} \cdot \mathbf{b}) = \begin{cases} m^n & \text{if } \mathbf{a} = \mathbf{0}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore,

$$\begin{aligned}\frac{1}{m^n}\sum_{\mathbf{b}\in\mathbb{Z}_m^n}\mathrm{WH}_{s,m^n}(\mathbf{b})\overline{\pi(\mathbf{b},h)} &= \frac{1}{m^n}\sum_{\mathbf{b}\in\mathbb{Z}_m^n}\left(\sum_{t=0}^{m^n-1}\chi(s_t)\overline{\chi(\mathbf{b}\cdot\mathbf{t})}\right)\left(\sum_{\tau=0}^{m^n-1}\chi(\mathbf{b}\cdot\boldsymbol{\tau})\overline{\omega(h\tau)}\right)\\ &= \frac{1}{m^n}\sum_{t,\tau=0}^{m^n-1}\chi(s_t)\overline{\omega(h\tau)}\sum_{\mathbf{b}\in\mathbb{Z}_m^n}\chi(\mathbf{b}\cdot(\boldsymbol{\tau}-\mathbf{t}))\\ &= \sum_{t=0}^{m^n-1}\chi(s_t)\overline{\omega(ht)},\end{aligned}$$

from which (5) follows.

Next we obtain upper bounds for $\sum_{\mathbf{b}}|\pi(\mathbf{b},h)|$. We will use the following representation:

$$\sum_{\mathbf{b}\in\mathbb{Z}_m^n}|\pi(\mathbf{b},h)| = \prod_{k=0}^{n-1}\sum_{a=0}^{m-1}\frac{|1-\omega(m^{k+1}h)|}{|1-\chi(a)\omega(m^kh)|}, \tag{6}$$

where the fraction

$$\frac{|1-\omega(m^{k+1}h)|}{|1-\chi(a)\omega(m^kh)|} = \frac{\left|\sin\frac{\pi m^{k+1}h}{r}\right|}{\left|\sin\left(\frac{\pi a}{m}+\frac{\pi m^kh}{r}\right)\right|}$$

is set to m if $\chi(a)\omega(m^kh)$ (and consequently $\omega(m^{k+1}h)$) is equal to 1.

To verify (6), observe that

$$\begin{aligned}\overline{\chi(\mathbf{b}\cdot\boldsymbol{\tau})} &= \chi(-b_0\tau_0-b_1\tau_1-\ldots-b_{n-1}\tau_{n-1}) = \chi(-b_0)^{\tau_0}\chi(-b_1)^{\tau_1}\ldots\chi(-b_{n-1})^{\tau_{n-1}},\\ \omega(h\tau) &= \omega(h(\tau_0+m\tau_1+\ldots+m^{n-1}\tau_{n-1})) = \omega(h)^{\tau_0}\omega(mh)^{\tau_1}\ldots\omega(m^{n-1}h)^{\tau_{n-1}}\end{aligned}$$

and therefore

$$\begin{aligned}\pi(\mathbf{b},h) &= \sum_{\boldsymbol{\tau}\in\mathbb{Z}_m^n}\prod_{k=0}^{n-1}\left(\chi(-b_k)\omega(m^kh)\right)^{\tau_k}\\ &= \prod_{k=0}^{n-1}\left(1+\chi(-b_k)\omega(m^kh)+(\chi(-b_k)\omega(m^kh))^2+\ldots+(\chi(-b_k)\omega(m^kh))^{m-1}\right)\\ &= \prod_{k=0}^{n-1}\frac{1-(\chi(-b_k)\omega(m^kh))^m}{1-\chi(-b_k)\omega(m^kh)} = \prod_{k=0}^{n-1}\frac{1-\omega(m^{k+1}h)}{1-\chi(-b_k)\omega(m^kh)},\end{aligned}$$

from which (6) follows.

For real x, introduce the function

$$\varphi(x) = \sum_{a=0}^{m-1}\frac{|\sin mx|}{\left|\sin\left(\frac{\pi a}{m}+x\right)\right|},$$

where we set $\varphi(\pi k/m) = m$ for $k = 0, \pm1, \ldots$ to make $\varphi(x)$ continuous. With these conventions, the internal sum in the right-hand side of (6) turns into $\varphi(\pi m^kh/r)$.

If $y \in \left[-\frac{\pi}{2m}, \frac{\pi}{2m}\right]$, then

$$\begin{aligned}\varphi\left(\frac{\pi}{2m}+y\right) &= \sum_{a=0}^{m-1} \frac{\cos my}{\sin\left(\frac{\pi(2a+1)}{2m}+y\right)} \\ &= \frac{1}{2}\sum_{a=0}^{m-1}\left(\frac{\cos my}{\sin\left(\frac{\pi(2a+1)}{2m}+y\right)} + \frac{\cos my}{\sin\left(\frac{\pi(2a+1)}{2m}-y\right)}\right) \\ &= \sum_{a=0}^{m-1} \frac{\cos my \cos y \sin\frac{\pi(2a+1)}{2m}}{\cos^2 y - \cos^2\frac{\pi(2a+1)}{2m}}.\end{aligned}$$

Applying here the inequality (2) and using the fact that $\varphi(x)$ is periodic with period $\frac{\pi}{m}$, we get

$$\varphi(x) \le \sum_{a=0}^{m-1} \csc\frac{\pi(2a+1)}{2m}.$$

This yields

$$\sum_{\mathbf{b}\in\mathbb{Z}_m^n} |\pi(\mathbf{b},h)| = \prod_{k=0}^{n-1} \varphi(\pi m^{k+1}h/r) \le (mS(m))^n, \tag{7}$$

which with (5) proves the first part of the Theorem.

If $m = 2$, then

$$\varphi(x) = 2(|\sin x| + |\cos x|) = 2\sqrt{1+|\sin 2x|}.$$

It is easy to check that

$$\varphi(x) \le 2\sqrt{2}, \quad (\varphi(x))^2\varphi(2x) \le (1+\sqrt{3})^3$$

for all real x. Hence,

$$\begin{aligned}\sum_{\mathbf{b}\in\mathbb{Z}_m^n} |\pi(\mathbf{b},h)| &= \left(\varphi(\pi h/r)(\varphi(\pi 2^{n-1}h/r))^2 \prod_{k=0}^{n-2}(\varphi(\pi 2^k h/r))^2\varphi(\pi 2^{k+1}h/r)\right)^{1/3} \\ &\le \begin{cases} 2\sqrt{2}(1+\sqrt{3})^{n-1} & \text{always,} \\ (1+\sqrt{3})^n & \text{if } 2^n \equiv 1 \pmod r, \end{cases}\end{aligned} \tag{8}$$

from which the second part of the Theorem follows.

Note that the upper bound in (7) is tight for odd m, even r, and $h = r/2$. The upper bound in (8) is tight for even n, $r = 2^n - 1$, and $h = r/3, 2r/3$.

3. Remarks

Let $\lceil m^n/2 \rceil \le r \le m^n$. Using the identity

$$\sum_{h=0}^{r-1} \omega(hj) = \begin{cases} r & \text{if } j \equiv 0 \pmod r, \\ 0 & \text{otherwise,} \end{cases}$$

we obtain

$$\begin{aligned}\frac{1}{r}\sum_{h=0}^{r-1}\mathrm{F}_{s,r}(h)\pi(\mathbf{b},h) &= \frac{1}{r}\sum_{h=0}^{r-1}\left(\sum_{t=0}^{r-1}\chi(s_t)\overline{\omega(ht)}\right)\left(\sum_{\tau=0}^{m^n-1}\overline{\chi(\mathbf{b}\cdot\boldsymbol{\tau})}\omega(h\tau)\right)\\ &= \frac{1}{r}\sum_{t=0}^{r-1}\left(\sum_{\tau=0}^{r-1}+\sum_{\tau=r}^{m^n-1}\right)\chi(s_t)\overline{\chi(\mathbf{b}\cdot\boldsymbol{\tau})}\sum_{h=0}^{r-1}\omega(h(\tau-t))\\ &= \sum_{t=0}^{r-1}\chi(s_t)\overline{\chi(\mathbf{b}\cdot\mathbf{t})}+\sum_{\tau=r}^{m^n-1}\chi(s_{\tau-r})\overline{\chi(\mathbf{b}\cdot\boldsymbol{\tau})}.\end{aligned}$$

Therefore,

$$|\,\mathrm{WH}_{s,m^n}(\mathbf{b})| \le 2|m^n-r| + \frac{1}{r}\max_{0\le h\le r-1}|\,\mathrm{F}_{s,r}(h)|\sum_{h=0}^{r-1}|\pi(\mathbf{b},h)|, \tag{9}$$

the estimate that is similar to (5). It is easy to check that (9) holds also for $r > m^n$.

To obtain from (9) estimates for the Walsh–Hadamard coefficients via the Fourier ones, we must find upper bounds for the sums $\sum_h |\pi(\mathbf{b},h)|$. This task seems to be more complicated than the estimation of $\sum_{\mathbf{b}} |\pi(\mathbf{b},h)|$, since there is no such simple representation for $\sum_h |\pi(\mathbf{b},h)|$ as (6).

References

[1] N. Ahmed and K. R. Rao, *Orthogonal Transforms for Digital Signal Processing*, Springer–Verlag, New York (1975).

[2] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties, *Journal of Combinatorial Theory*, Ser. A, Vol. 40 (1985), pp. 90–107.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, in Encyclopedia of Mathematics and Its Applications, Vol. 20, Addison–Wesley, Reading MA (1983).

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North–Holland, Amsterdam (1977).

[5] D. Maslen and D. Rockmore, Generalized FFTs – a survey of some recent results, *Proceedings of IMACS Workshop in Groups and Computation*, Vol. 28 (1995), pp. 182–238.

[6] O. S. Rothaus, On "bent" functions, *Journal of Combinatorial Theory*, Ser. A, Vol. 20 (1976), pp. 300–305.