Fast quantum Fourier–Weyl–Heisenberg transforms

Valeri G. Labunets, Ekaterina V. Rundblad-Labunets, and Jaakko Astola

Department of Automation and Information Technologies, Urals State Technical University, Ekaterinburg, Russia

Signal Processing Laboratory, Tampere University of Technology, Tampere, Finland

ABSTRACT

We study the Fourier harmonic analysis of a functions on discrete 1D and nD Heisenberg–Weyl groups $\mathcal{HW}_3[K, K, K]$ and $\mathcal{HW}_{2n+1}[K^n, K^n, K]$, where $K := \text{GF}(2)$, $\text{GF}(2^m)$, $\text{GF}(p)$, $\text{GF}(p^m)$ are the Galois fields, and develop fast quantum Fourier–Heisenberg–Weyl transforms on this groups.

Keywords: quantum computer, fast algorithms, Fourier transforms, non–commutative groups

1. INTRODUCTION

Up to now almost all the groups considered for applications to signal processing are Abelian groups. Fast Fourier Transforms (FFTs) on finite Abelian groups are widely used in signal processing and experimental research. The modern theory of such transforms is of increasing interest, and many fundamental problems in particular applications can be solved already. The quantum Fourier transform (QFT) on Abelian groups, a quantum analog of the classical Fourier transform, has been shown to be a powerful tool in developing quantum algorithms. However, in classical signal processing literature, there are the proofs for the existence of FFTs for dihedral and quaternion groups, for extra–special 2–groups, for solvable and metabelian group, for metacyclic groups, for Heisenberg–Weyl groups. The report of Stancovic, Morago, and Astola, the books of Beth, Clausen, and Baum and the survey article are references for the computational aspects of these transforms.

Groups that have received great interest in the signal processing and physics community are Heisenberg–Weyl groups (because of their connection to time–frequency Wigner methods and Weyl calculus). In this paper we study the harmonic analysis of functions on discrete 1D and nD Heisenberg–Weyl groups $\mathcal{HW}_3[K, K, K]$ and $\mathcal{HW}_{2n+1}[K^n, K^n, K]$, where $K := \text{GF}(2)$, $\text{GF}(2^m)$, $\text{GF}(p)$, $\text{GF}(p^m)$ are the Galois fields, and develop fast quantum Fourier–Heisenberg–Weyl transforms on noncommutative groups.

Now recall the following group theoretical explanation of the Fourier transform on noncommutative groups. Theoretical algebraic details can be found in.

Further author information:
V.G.L.E.V.R.–L, E-mail: lab@cs.tut.fi, J. A. E-mail: jta@cs.tut.fi
The elements \( \{ t_{ij}^\alpha(g) \}_{i,j=1}^{s} \) form an orthogonal basis in the space \( L(G, C) \) of \( C \)-valued functions defined on \( G \):

\[
(n_\alpha/|G|) \sum_{g \in G} T_{ij}^\alpha(g)T_{mi}^\beta(g) = \delta_\alpha^\beta \delta_{im} \delta_{jl}.
\]

and any function \( f(g) \in L(G, C) \) can be expanded into a Fourier series

\[
f(g) = \sum_{\alpha=1}^{s} \sum_{i=1}^{n_\alpha} \sum_{j=1}^{n_\alpha} n_\alpha F_{ij}(\alpha)T_{ij}^\alpha(g^{-1}), \quad \text{where} \quad F_{ij}(\alpha) = \frac{1}{|G|} \sum_{g \in G} f(g)T_{ij}^\alpha(g).\tag{1}
\]

In this case one speaks about the harmonic synthesis and harmonic analysis of a function \( f(g) \), respectively. In matrix notation this expression has the following form:

\[
f(g) = \sum_{\alpha=1}^{s} n_\alpha \text{tr}[\hat{F}(\alpha)\hat{T}^\alpha(g)], \quad \text{where} \quad \hat{F}(\alpha) = \frac{1}{|G|} \sum_{g \in G} f(g)\hat{T}^\alpha(g).\tag{2}
\]

Here, \( \hat{F}(\alpha) \) is the matrix–valued spectrum of \( f(g) \) (see Fig. 1) and \( \text{tr}[:]=\) denotes the matrix trace. These expressions are called the direct and inverse \( G \)-Fourier transforms on the group \( G \). If \( G \) is the Heisenberg–Weyl group \( \mathcal{HW}_{2n+1}(K^n, K^n, K) \) over a commutative ring \( K \), then we call them the Fourier–Heisenberg–Weyl transforms.

**Definition 1.3.** If complex–valued functions \( k(g), \ x(g): G \rightarrow C \) are defined on the group \( G \), then expressions

\[
y(g) = (k*x)(g) = \frac{1}{|G|} \sum_{h \in G} k(g \star h^{-1})x(h), \quad \text{cor}[k,x](h) = (k \star x)(q) = \frac{1}{|G|} \sum_{g \in G} k(g \star h^{-1})x(g)
\]

are called the \( G \)-convolution and \( G \)-cross correlation on the group, respectively.

**Theorem 1.4.** The direct \( G \)-Fourier transform maps the \( G \)-convolution and \( G \)-cross correlation into the product of matrix–valued spectra (see Fig. 2): \( \hat{Y}(\alpha) = \hat{K}(\alpha)\hat{X}(\alpha) \), \( \text{COR}(\alpha) = \hat{K}^\dagger(\alpha)\hat{X}(\alpha) \), respectively, where \( ^\dagger \) denote the Hermitian conjugate.

We can present the \( G \)-Fourier transform as \((s \times |G|)\)-matrix of \( s \times n_\alpha \)-matrix–valued harmonics \( \hat{T}^\alpha(g) \) (\( \alpha = 0, 1, \ldots, s \)):
Figure 2. $G$–Fourier transformation of $G$–convolution and $G$–correlation

\[
\mathcal{F}_{s \times |G|} := \begin{bmatrix}
    \mathcal{T}_{m_1 \times m_1}^1 (g) \\
    \mathcal{T}_{m_2 \times m_2}^2 (g) \\
    \vdots \\
    \mathcal{T}_{m_s \times m_s}^s (g)
\end{bmatrix} = \begin{bmatrix}
    \begin{array}{ccc}
        & & \\
        & \bigcirc & \\
        & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        & & \\
        & \bigcirc & \\
        & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
    \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
    \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
\end{bmatrix}.
\] (3)

This matrix is represented as $|G \times G|$–matrix

\[
\mathcal{F}_{|G| \times |G|} = \begin{bmatrix}
    \begin{array}{ccc}
        & & \\
        & \bigcirc & \\
        & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        & & \\
        & \bigcirc & \\
        & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
    \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
    \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} & \ldots & \begin{array}{ccc}
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
        \bigcirc & \bigcirc & \bigcirc \\
    \end{array} \\
\end{bmatrix}.
\] (4)

because $n_1^2 + n_2^2 + \ldots + n_s^2 = |G|$ is valid. Our main purpose is to find the fast Fourier transform for this matrix for the Heisenberg–Weyl group. Different symbols show different scalar–valued elements in both matrices (3) and (4).

2. HEISENBERG–WEYL GROUPS

We will investigate the Fourier–Heisenberg–Weyl transform on the $n$D Heisenberg–Weyl group with elements over a commutative finite ring $K$

\[
\mathcal{HW}_{2n+1} = \mathcal{HW}_{2n+1} (K^n, K^n, K) := \left\{ g(t, \omega, c) = \begin{bmatrix} 1 & \omega & c \\ \omega & 1 & t \end{bmatrix} \bigg| t, \omega \in K^n, c \in K \right\}
\]

consisting of upper triangular $((n + 2) \times (n + 2))$–matrices $g(t, \omega, c)$ with the following multiplication rule:

\[
g(t_1, \omega_1, c_1) \cdot g(t_2, \omega_2, c_2) = g(t_1 + t_2, \omega_1 + \omega_2, c_1 + c_1 + \langle t_1 | \omega_2 \rangle),
\] (5)

where $K^n := K \oplus K \oplus \ldots \oplus K$ is a $n$–D vector space over $K$ and $\langle t | \omega \rangle := t_1 \omega_1 + t_2 \omega_2 + \ldots + t_n \omega_n$ denotes the inner product of $n$D vectors $t$ and $\omega$. Every group element $g(t, \omega, c)$ has the inverse $g^{-1}(t, \omega, c) = g(-t, -\omega, -c - \langle t | \omega \rangle)$. 
The groups $\mathcal{H}W_3(K, K, K)$ and $\mathcal{H}W_{2n+1}(K^n, K^n, K)$ consist of $|K|^3$ and $|K|^{2n+1}$ elements, respectively. Let us now introduce the following generators:

$$ T := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = g(1, 0, 0), \quad \Omega := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = g(0, 1, 0), \quad C := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = g(0, 0, 1), \quad I := \begin{bmatrix} 1 & 1 \end{bmatrix} = g(0, 0, 0) $$

for $\mathcal{H}W(3, K, K)$. It is easy to check that

$$ T^t = \begin{bmatrix} 1 & t \\ 1 & 1 \end{bmatrix} = g(t, 0, 0), \quad \Omega^\omega = \begin{bmatrix} 1 & \omega \\ 1 & 1 \end{bmatrix} = g(0, \omega, 0), \quad C^c = \begin{bmatrix} 1 & c \\ 1 & 1 \end{bmatrix} = g(0, 0, c), \quad g(t, \omega, c) = T^t \Omega^\omega C^c = \begin{bmatrix} 1 & \omega & c \\ 1 & 1 & 1 \end{bmatrix}. $$

Analogously, we introduce the following generators for $\mathcal{H}W_{2n+1}(K^n, K^n, K)$:

<table>
<thead>
<tr>
<th>$T_i^t$</th>
<th>$\Omega_i^\omega$</th>
<th>$C^c$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$1 \ldots 0 \ldots 0$</td>
<td>$1 \ldots t_j \ldots 1$</td>
<td>$1 \ldots c \ldots 0$</td>
</tr>
<tr>
<td>$1 \ldots 0 \ldots 1$</td>
<td>$1 \ldots 0 \ldots 0$</td>
<td>$1 \ldots 1 \ldots 0$</td>
</tr>
</tbody>
</table>

where $i = 1, 2, \ldots, n$. Then, we have $g(t_1, \ldots, t_n, (\omega_1, \ldots, \omega_n), c) = (T_1^t \ldots T_n^t)(\Omega_1^\omega \ldots \Omega_n^\omega)C^c := T^t \Omega^\omega C^c$, where $T^t := T_1^t \ldots T_n^t$, $\Omega^\omega := \Omega_1^\omega \ldots \Omega_n^\omega$. This means that every element $g(t, \omega, c)$ has the unique representation of the form $g(t, \omega, c) = T^t \Omega^\omega C^c$. In particular, we see that $\Omega_i^\omega T_j^t = \Omega_j^\omega T_i^t$, $T_i^t C^c = C^t T_i^t$, $\Omega^\omega C^c = C^\omega \Omega^\omega$, $\Omega^\omega T^t \Omega^\omega = C^{-\omega(t)}$, that is, all elements of the form $C^c$ commute with all elements of the Heisenberg–Weyl group and, hence, they are contained in its commutator subgroup.

For simplicity let us introduce the following notation $\mathcal{H}W := \mathcal{H}W_{2n+1}(K^n, K^n, K)$. Theorem 2.1.17

**Theorem 2.1.17** The commutator subgroup $[\mathcal{H}W, \mathcal{H}W]$ and the center of the Heisenberg–Weyl group $\mathcal{H}W$ are equal and both are isomorphic to the additive group $AK$ of the ring $K$ : $[\mathcal{H}W, \mathcal{H}W] = Z(\mathcal{H}W) \sim \langle C \rangle \sim AK$. Let us find conjugated the classes $\mathcal{H}W \circ \mathcal{H}W \circ \mathcal{H}W^{-1}$. For this, we calculate (in the general form) the following products $(T^t \Omega^\omega C^c)$, $(T^t \Omega^\omega C^\omega)$, $(T^{-t} \Omega^{-\omega} C^{-c} + (\omega(t))$. The product of the first two triples gives: $(T^t + t_0) (\Omega^\omega + \omega(t) C^c + c + (\omega(t)) \Omega^{-\omega} C^{-c} - (\omega(t))$. The product of the second two triples gives $T^t \Omega^\omega C^\omega + (\omega(t)) + (t_0 \omega)$. Hence, an arbitrary fixed element $T^t \Omega^\omega C^\omega$ runs the following orbit (conjugate class):

$$ \mathcal{H}W \circ (T^t \Omega^\omega C^\omega) \circ \mathcal{H}W \rightarrow \left\{ T^t \Omega^\omega C^\omega + (\omega(t)) + (t_0 \omega) \mid \omega, b \in K^n \right\}. $$

If $t_0 = \omega_0 = 0$ then every element $C^c$ is mapped in itself: $\mathcal{H}W \circ (C^c) \circ \mathcal{H}W \rightarrow \{ C^c \}$. Each such element forms a separate class $\{ C^c \}$, and all such elements $C^c$ generates $|K|$ classes $\{ C^c \}_{K^{\omega-1}}$.  

If $a_0 = 0$ then we have $\mathcal{H}W \bullet (t_0^* \Omega^{0}) \bullet \mathcal{H}W \rightarrow \{ T_{t_0}^* \Omega^{0} C(\omega |t_0) = - \langle t | \omega \rangle \mid \omega, b \in \mathbb{K}^n \}$, and every element $T_{t_0}^* \Omega^{0}$ runs an orbit consisting of the elements of the form $T_{t_0} T_{\omega} C(\omega |t_0) = - \langle t | \omega \rangle$, where $\omega, t \in \mathbb{K}^n$. In general case, this orbit depends on a type of the ring $\mathbb{K}$. We will consider the Heisenberg–Weyl group of the following type $\mathcal{H}W_{2n+1}(\mathbb{K}^n, \mathbb{K}^n, \mathbb{K})$, where $\mathbb{K}$ is the Galois field $\mathbb{GF}(p)$. In this case, we have $p$ single–element orbits $\{ C_{\alpha} \}_{\alpha=0}^{p-1}$. So as in this case linear combination $\langle \omega |t_0 \rangle - \langle t | \omega \rangle = c$ runs all elements of the Galois field for any pair $\omega_0, t_0 \in \mathbb{GF}(p)$, then there are $p^{2n} - 1$ such orbits. The total number $s$ of conjugated classes of the Heisenberg–Weyl group $\mathcal{H}W_{2n+1}(\mathbb{GF}(p), \mathbb{GF}(p), \mathbb{GF}(p))$ equals to $s = p^{2n} + p - 1$. Hence the dimensions $n_\alpha$ of irreducible representations (matrix–valued harmonics) must satisfy to the equation $\sum_{\alpha=1}^{p^{2n}+p-1} n_\alpha^2 = p^{2n} + 1$ in the considered case.

It is known\textsuperscript{17} that 1D irreducible representations of the Heisenberg–Weyl group $\mathcal{H}W_{2n+1}(\mathbb{GF}(p), \mathbb{GF}(p), \mathbb{GF}(p))$ coincide with $p^{2n}$ characters of the Abelian group $\mathcal{H}W/[\mathcal{H}W, \mathcal{H}W] \sim \mathbb{AGF}(p) \oplus \mathbb{AGF}(p)$:

$$T^{\alpha_1, \alpha_2} (T^t \Omega^w C^c) = \chi_{\alpha_1, \alpha_2} ([T^t \Omega^w]) = \varepsilon_{\alpha_1} (\omega_1 | t_1) + \omega_2 | \alpha_2 \rangle,$$

(6)

where $\alpha_1 := (\alpha_1^1, \alpha_1^2, ..., \alpha_1^p)$, $\alpha_2 = (\alpha_2^1, \alpha_2^2, ..., \alpha_2^p) \in [\mathbb{AGF}(p)]^n$, $\varepsilon_p = \sqrt{1}$ $\in \mathbb{C}$. Hence, $\sum_{\alpha_1=1}^{p^{2n}} n_\alpha^2 = p^{2n+1} - p^{2n} = p^2(p-1)$. As $n_\alpha \mid p^{2n+1}$ then all $n_\alpha$ must be equal to $p$. Thus, the Heisenberg–Weyl group $\mathcal{H}W = \mathcal{H}W_{2n+1}(\mathbb{GF}(p), \mathbb{GF}(p), \mathbb{GF}(p))$ has $p-1$ $p^n\mathbb{D}$ irreducible representations. The 1D and $p^n\mathbb{D}$ irreducible representations exhaust all irreducible representations of the group $\mathcal{H}W$ because $\sum_{\alpha=1}^{p^{2n}} n_\alpha^2 = p^{2n+1} - p^{2n} = p^{2n+1} - p^{2n}$. Hence, an arbitrary signal $f (g) : \mathcal{H}W_{2n+1}(\mathbb{GF}(p), \mathbb{GF}(p), \mathbb{GF}(p)) \rightarrow \mathbb{C}$ defined on the Heisenberg group and with values in $\mathbb{C}$ has $p^{2n}$ complex–valued and $p-1$ $(p^n \times p^n)$–matrix–valued spectral components (see fig. 3).

Let us first consider the simple case $n = 1$. In this case the Heisenberg–Weyl group $\mathcal{H}W_{3}(\mathbb{GF}(p), \mathbb{GF}(p), \mathbb{GF}(p))$ has $p-1 pd$ representations:

$$\hat{T}_{p^3} (T^t \Omega^w C^c) = \hat{T}_{p^3} (T^t) \hat{T}_{p^3} (\Omega^w) \hat{T}_{p^3} (C^c) = \hat{S}_{p^t} \hat{D}_{p^w} \hat{C}_{p^c},$$

(7)

where

$$\hat{T}_{p^3} (T^t) = \hat{S}_{p^t} = \begin{bmatrix}
\cdot & 1 \\
\cdot & \ddots & 1 \\
\cdot & \cdots & \cdot & 1
\end{bmatrix}, \quad \hat{T}_{p^3} (\Omega^w) = \hat{D}_{p^w} = \begin{bmatrix}
\varepsilon_{p^0} & \cdots & \varepsilon_{p^{p-1}} \\
\varepsilon_{p^1} & \ddots & \varepsilon_{p^{p-1}} \\
\varepsilon_{p^2} & \cdots & \varepsilon_{p^{p-1}}
\end{bmatrix}, \quad \hat{T}_{p^3} (C^c) = \hat{C}_{p^c}.
$$

From (6) and (7) we have the following expressions for Fourier transform on this Heisenberg–Weyl group:

- matrix–valued spectrum

$$\hat{F}_{p \times p} (\alpha_3) = \sum_{t, \omega, c \in \mathbb{GF}(p)} f(t, \omega, c) \hat{S}_{p} \hat{D}_{p} \hat{C} \varepsilon_{\alpha_3 \omega} \varepsilon_{\alpha_3 c} = \sum_{t, \omega, c \in \mathbb{GF}(p)} f(t, \omega, c) \left[ \begin{array}{ccc}
\cdot & 1 \\
\cdot & \ddots & 1 \\
1 & \cdots & 1
\end{array} \right] \left[ \begin{array}{ccc}
\varepsilon_{p^0} & \cdots & \varepsilon_{p^{p-1}} \\
\varepsilon_{p^1} & \ddots & \varepsilon_{p^{p-1}} \\
\varepsilon_{p^2} & \cdots & \varepsilon_{p^{p-1}}
\end{array} \right] \hat{D}_{p} \hat{C} \varepsilon_{\alpha_3 \omega} \varepsilon_{\alpha_3 c},$$

(8)
• scalar–valued spectrum

\[ F(\alpha_1, \alpha_2) = \sum_{t, \omega, c} \sum_{\epsilon_p} \sum_{\epsilon} f(t, \omega, c) \epsilon_p^{\alpha_1 t} \epsilon_p^{\alpha_2 \omega}. \]  

(9)

We construct the Fourier transform matrix \( FHW \) (4) in the following way: the matrix columns will be enumerated with elements of this group. The column with the number \( n = t + \omega p + t^2 \) corresponds to the element \( T^t \Omega^\omega C^c \), \( t, \omega, c = 0, 1, \ldots, p - 1 \). The rows of the matrix \( FHW \) are ordered according to expressions (9) and (8). Then

\[
FHW = 
\begin{bmatrix}
\epsilon^0(F_p \otimes F_p) & \epsilon^0(F_p \otimes F_p) & \ldots & \epsilon^0(F_p \otimes F_p) \\
\epsilon^0(F_p \otimes I_p) & \epsilon^1(F_p \otimes I_p) & \ldots & \epsilon^{p-1}(F_p \otimes I_p) \\
\ldots & \ldots & \ldots & \ldots \\
\epsilon^0(F_p \otimes I_p) & \epsilon^{p-1}(F_p \otimes I_p) & \ldots & \epsilon^1(F_p \otimes I_p)
\end{bmatrix}
\]

(10)

where \( F_p \otimes F_p \) is the 2D transform (9) and \( \epsilon^i(F_p \otimes I_p) \) is 2D transform (8). The expression (10) is the fast classical Fourier–Heisenberg–Weyl transform.\(^{10,12}\)

Let us consider now the \( n \)D Heisenberg–Weyl group \( \mathcal{HW}_{2n+1}(GF^n(p), GF^n(p), GF(p)) \). This group has \( p^{2n} \) 1D irreducible representations (6). We construct \( p-1 \) \( p^D \) representations of this group by the following way. Let

\[
\hat{T}_{p^3}^{\alpha_3}(T^t \Omega^\omega C^c) = \hat{T}_{p^3}^{\alpha_3}(T^t) \hat{T}_{p^3}^{\alpha_3}(\Omega^\omega) \hat{T}_{p^3}^{\alpha_3}(C^c) := \left[ \bigotimes_{i=1}^{n} \hat{T}_{p}^{\alpha_3}(T^t) \right] \left[ \bigotimes_{i=1}^{n} \hat{T}_{p}^{\alpha_3}(\Omega^\omega) \right] \left[ \hat{T}_{p}^{\alpha_3}(C^c) \right] = \]

\[
= [\hat{S}_{p}^{\alpha_3 t} \otimes \ldots \otimes \hat{S}_{p}^{\alpha_3 t}][\hat{D}_{p}^{\alpha_3 \omega} \otimes \ldots \otimes \hat{D}_{p}^{\alpha_3 \omega}][\epsilon_p \hat{I}_{p^n}]^{\alpha_3 c}. \]  

(11)

It is elementary exercise to verify that these representations are irreducible non–equivalent representations of the \( n \)D Heisenberg–Weyl group \( \mathcal{HW}_{2n+1}(GF^n(p), GF^n(p), GF(p)) \). From (11) we obtain

\[
FHW = \left[ (F_p^n \otimes F_p^n) \oplus (I_p \otimes F_p^n \otimes I_p^n) \right] \left[ F_p \otimes I_{p^n} \right] = \left[ I_p^{n-2} \oplus (I_p \otimes F_p^n) \right][I_p \otimes F_p \otimes I_{p^n}][F_p \otimes I_{p^n} \otimes I_{p^n}], \]  

(12)

where \( F_p^n := F_p \otimes F_p \oplus \ldots \oplus F_p = \prod_{i=1}^{n} [I_p \otimes F_p \otimes I_{p^{-1}}] \) is the discrete \( n \)D Fourier transform matrix. Expression (12) is a fast Fourier–Heisenberg transform (FFHT) for the group \( \mathcal{HW}_{2n+1}(GF^n(p), GF^n(p), GF(p)) \).
3. QUANTUM FOURIER–HEISENBERG–WEYL TRANSFORMS

We begin by setting some notations. Let $\text{SYST} = \mathcal{Q}_m$ be a deterministic system or an automaton with finite set of states $\mathcal{Q}_m := \{q \mid q = 0, 1, 2, \ldots, m - 1\}$. These states are called the classical or deterministic states. We can represent these states by means of basis vectors in $m$D space $\mathbb{R}^m$:

$$|q\rangle := \begin{cases} |0\rangle &:= (1, 0, \ldots, 0)^t = e_0, \text{ if } q = 0, \\ |1\rangle &:= (0, 1, \ldots, 0)^t = e_1, \text{ if } q = 1, \\ \vdots &\vdots \\ |m-1\rangle &:= (0, 0, \ldots, 1)^t = e_{m-1}, \text{ if } q = m-1. \end{cases}$$

We use the Dirac braket notation to represent $m$D vector, where the ket–vector $\left| \cdot \right\rangle$ is analogous to a column vector, the bra–vector $\left\langle \cdot \right|$ is analogous to the complex conjugate transpose of the ket–vector, and the braket symbol $\left\langle \cdot \mid \cdot \right\rangle$ is the inner product in $\mathbb{R}^m$. The simplest finite set of states is $\mathcal{Q}_2 = \{q \mid q = 0, 1\}$. Two–state systems are basic unit of storage in classical computers and are called the trigger, flip–flop or the classical bit ($\text{CL–BIT}$). Analogously, $m$–states system is called $m$–states trigger or classical mit ($\text{CL–MIT}$). The classical information theory is based on the classical bit as a fundamental atom. For CL–BIT we have the following vector representation of states in 2D space $\mathbb{R}^2$:

$$|q\rangle := \begin{cases} |0\rangle &:= (1, 0)^t = e_0, \text{ if } q = 0, \\ |1\rangle &:= (0, 1)^t = e_1, \text{ if } q = 1. \end{cases}$$

A collection of $n$ CL–MIT $\begin{bmatrix} q_1 & q_2 & \cdots & q_n \end{bmatrix}$ is called the classical n–digital m–register (or CL–$m^n$REG), and a collection of the $n$ CL–BIT is called the classical n–digital 2–register (or CL–2$^n$REG). Information is stored in the registers in $q$–ary form. The states of $m^n$REG can be represented by $m^n$ basis vectors $|q_1\rangle \otimes |q_2\rangle \otimes \cdots \otimes |q_n\rangle = |(q_1, q_2, \ldots, q_n)\rangle = |q\rangle$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle := |0, 0, \ldots, 0\rangle = |0\rangle,$$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle := |0, 0, \ldots, 1\rangle = |1\rangle,$$

$$\vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots,$$

$$|m-1\rangle \otimes \cdots \otimes |m-1\rangle := |m-1, m-1, \ldots, m-1\rangle = |m^n - 1\rangle$$

in $m^n$D space $\mathbb{R}^{m^n}$ that is the tensor product of $n$ mD spaces $\mathbb{R}^{m^n} := \mathbb{R}^m \otimes \mathbb{R}^m \otimes \cdots \otimes \mathbb{R}^m$. For example, number 7 is represented by a CL–3$^3$REG in state $|(0, 2, 1)\rangle$. Analogously, the states of CL–$2^n$REG can be represented by $2^n$ base vectors $|q_1\rangle \otimes |q_2\rangle \otimes \cdots \otimes |q_n\rangle = |(q_1, q_2, \ldots, q_n)\rangle = |q\rangle$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle := |0, 0, \ldots, 0\rangle = |0\rangle,$$

$$|0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle := |0, 0, \ldots, 1\rangle = |1\rangle,$$

$$\vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots \vdots,$$

$$|1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle := |1, 1, \ldots, 1\rangle = |2^n - 1\rangle,$$

in $2^n$D space $\mathbb{R}^{2^n} := \mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \cdots \otimes \mathbb{R}^2$. Note that any superposition of two distinct classical states is not a legitimate classical state.

The quantum system theory describes behavior of quantum systems $\text{SYST}_{qu}$. We restrict our attention to quantum systems $\text{SYST}_{qu}$ having finite classical state sets. For a given quantum system, we denote the classical state set by the same symbol $\mathcal{Q}_m = \{q \mid q = 0, 1, \ldots, m-1\}$. A quantum state of quantum finite state systems $\text{SYST}_{qu}$ is represented by means of $m$ complex numbers $\varphi_0, \varphi_1, \ldots, \varphi_{m-1}$, where $|\varphi_q|^2 = p_q$ is the probability quantum system being in the state $q$. These complex numbers are called the quantum probabilities or amplitudes. Hence, the quantum state can be represented by a $m$D complex–valued vector $|\varphi\rangle = (\varphi_0, \varphi_1, \ldots, \varphi_{m-1})^t$ such that

$$||\varphi||^2 = \langle\varphi|\varphi\rangle = \sum_{q=0}^{m-1} |\varphi_q|^2 = 1. \quad (13)$$

The $m$–state quantum systems are called the quantum mit (QU–MIT). It has a chosen “computational basis” $|0\rangle$, $|1\rangle$, $\ldots$, $|m-1\rangle$, corresponding to the classical $m$–ary values $0, 1, \ldots, m-1$. Obviously, the unit $m$D vectors $|\varphi\rangle$ belong to the unit sphere of the $m$D Hilbert space $\mathcal{H}_m := \mathbb{C}^m$. All these unit vectors $|\varphi\rangle \in \mathcal{H}_m$ are called the pure states of the quantum system. They form unit sphere $S_{m-1} \in \mathcal{H}_m$. With each classical state $q = 0, 1, \ldots, m-1$ we associate a
basis pure quantum state $|q⟩ = |0⟩ = (1, 0, \ldots, 0)^t$, $|1⟩ = (0, 1, \ldots, 0)^t$, \ldots, $|m−1⟩ = (0, \ldots, 0, 1)^t$. A classical system can be placed only in one of classical state in every moment of time, while the quantum system can be in all classical states simultaneously! One of the fundamental principles of quantum mechanics is the superposition principle which guarantees that any superposition of two distinct states is again a legitimate quantum state. For example, at the quantum level an electron can be placed a superposition of many different energies; however, in the classical realm this obviously cannot be. Hence, every quantum state may be specified by linear combinations of elements in the orthonormal basis $|q⟩ = |ϕ⟩ = \sum_{q=0}^{m−1} Ψ_q |q⟩$. This quantum state $|ϕ⟩$ contains all pure quantum states associated with classical states $|q⟩$. Such states are said to be placed the superposition of classical states. A quantum system is said to be coherent if it is a linear superposition of its basis states. A result of quantum mechanics is that if a system that is in a linear superposition of states interacts in any way with its environment, the superposition is destroyed. This loss of coherence is called decoherence. The values $Ψ_q$ are quantum probabilities, and $|Ψ_q|^2$ gives the probability of collapsing $|ϕ⟩$ into state $|q⟩$, if it decoheres. Note that the discrete wave function $Ψ_q$ describes a real physical system that must collapse to exactly one basis state. Therefore, the probabilities governed by the amplitudes $Ψ_q$ must sum to unit. This necessary constraint is expressed as the unitary condition (13).

Consider, for example, the “simplest” two-state quantum system (quantum trigger = quantum flip–flop = spin system = QU–BIT), whose basis states are usually represented as $|0⟩$ and $|1⟩$ or $|↑⟩$ and $|↓⟩$, respectively. In this system the discrete wave function $Ψ_q$ is a distribution over two values (spin up and spin down) and a coherent state $|ϕ⟩$ is a linear superposition of $|↑⟩$ and $|↓⟩$ (e.g., $|ϕ⟩ = Ψ_0 |0⟩ + Ψ_1 |1⟩ = Ψ_0 |↑⟩ + Ψ_1 |↓⟩$). As long as the system maintains its quantum coherence, it cannot be said to be either $↑$–state or $↓$–state. It is in some sense both at once. Classically, it must be one or the other, and when this system decoheres the result is, for example, the $|↑⟩$–state with probability $|⟨↑|Ψ(q)⟩|^2 = (|Ψ_0|^2) + (|Ψ_1|^2).

The quantum register QU–m\textsuperscript{n}REG\((q)\) := \left[\begin{array}{c} q_1 \\ q_2 \\ \vdots \\ q_n \end{array}\right]$ containing n quantum MITs has $m^n$ classical states $|q_1, q_2, \ldots, q_n⟩ = |q_1⟩⊗|q_2⟩⊗\cdots⊗|q_n⟩$ which are denoted by n digital $m$–ary numbers $q_1, q_2, \ldots, q_n \in \{0, 1, \ldots, m−1\}$. A quantum register of length n QU–mits is represented with a $m^n$–ary abelian group $\mathbb{C}^m^n := \mathbb{C}^m ⊗ \mathbb{C}^m \cdots ⊗ \mathbb{C}^m$. We shall index each classical state by n–tuple $|(q_1, q_2, \ldots, q_n)⟩$ or bold single–tuple $|q⟩$, where $q := (q_1, q_2, \ldots, q_n)$ is n–digital $m$–ary representation of the number q. A quantum state of a QU–m\textsuperscript{n}REG is represented by means of $m^n$ quantum probabilities $Ψ_q := Ψ(q_1, q_2, \ldots, q_n) : Ψ_0 := Ψ(0,0,\ldots,0), Ψ_1 := Ψ(0,0,\ldots,1), \ldots, Ψ_{M−1} := Ψ(m−1,m−1,\ldots,m−1)$, where $q_1, q_2, \ldots, q_n \in \{0, 1, \ldots, m−1\}$ and $M = m^n$. Hence, the quantum state can be represented in this way by a $m^n$ complex–valued vector

$|ϕ⟩ = \sum_{q=0}^{M−1} Ψ_q |q⟩ = \sum_{q_1=0}^{m−1} \sum_{q_2=0}^{m−1} \cdots \sum_{q_n=0}^{m−1} Ψ(q_1,q_2,\ldots,q_n) |(q_1,q_2,\ldots,q_n)⟩$, where each $Ψ_q = Ψ(q_1,\ldots,q_n)$ is a complex number. The squared absolute value of all the $Ψ_q$ values must sum to one.

All operations in quantum computation are realized by means of transformations on the QU–mits contained in a quantum register. The possible transformations a quantum computer can carry out are the elements of unitary group $U(\mathbb{C}^m^n)$. A quantum logic gate is an elementary quantum computing device which performs a fixed unitary transformation on selected QU–mits in a fixed period of time. A transformation gate takes an input quantum state and produces a modified output quantum state. The gates have the same number of inputs as outputs, and a gate of n inputs carries a unitary transformation of the group $U(\mathbb{C}^m^n)$, i.e., a generalized rotation in the Hilbert space $\mathbb{C}^m^n$. To study the complexity of performing unitary transformations on QU–m\textsuperscript{n}REG, we introduce two types of quantum logic gates18–21:

- **Local unitary operations** on QU–mit k are matrices of the form $U_m^{(k)} := I_{m−k} ⊗ U_m ⊗ I_{m−n−k}$, where $U_m$ is an element of the unitary group $U(\mathbb{C}^m^n)$ of (m × m)–matrices. For these operations we have

\[
\left[I_{m−k} ⊗ U_m ⊗ I_{m−n−k}\right]|q_1⟩ ⊗ \cdots ⊗ |q_k⟩ ⊗ \cdots ⊗ |q_n⟩ = |q_1⟩ ⊗ \cdots ⊗ \left[U_m |q_k⟩\right] ⊗ \cdots ⊗ |q_n⟩. \tag{14}
\]

- For any unitary $[m^n−k × m^n−k]$–transformation $U_{m−n−k}$ we define the n–mit transformation $U_{m−n−k}^{↑k}$ by

\[
U_{m−n−k}^{↑k} := I_{m^n−m−n−k} ⊗ U_{m^n−k}. \tag{15}
\]
tional steps are synchronised in time. The quantum network is the natural quantum generalization of the acyclic “output”.

In the quantum world, a complex–valued function

\[ f : \mathbb{Z}/m^n \to \mathbb{C} \]

will be viewed here as a quantum network (or a family of quantum networks). The output of some of the gates are connected by wires to the input of others and they interconnected without fanout or feedback by quantum wires. A quantum computer will be viewed here as a quantum network (or a family of quantum networks). Quantum computation is defined as unitary evolution of the network which takes its initial state “input” into some final state “output”.

In the quantum world, a complex–valued function \( f(t) : \mathbb{Z}/m^n \to \mathbb{C} \) can be represented by a superposition \( |f\rangle = \sum_{t=0}^{M-1} f(t)|t\rangle \) (perhaps normalized), where \( t = (t_1, t_2, \ldots, t_n) \in \mathbb{Z}/m^n, t_1, t_2, \ldots, t_n \in 0, 1, \ldots, m - 1 \) and \( M := m^n \). Note that in the quantum setting, the function on \( \mathbb{M} \) states is represented compactly as a superposition on \( \log_2 \mathbb{M} = n \) QU–MIs (I). The quantum Fourier transform (QFT) is a unitary operation that performs the DFT on the amplitude vector of a quantum state — the QFT maps the quantum state

\[ |f\rangle = \sum_{t=0}^{M-1} f(t)|t\rangle \to \text{the state } |F\rangle = \sum_{\omega=0}^{M-1} F(\omega)|\omega\rangle, \]

where

\[ F(\omega) := \frac{1}{M} \sum_{t=0}^{M-1} f(t) \exp(-2\pi t\omega/M), \quad f(t) := \sum_{\omega=0}^{M-1} F(\omega) \exp(2\pi t\omega/M). \]
We can calculate the spectrum $F(\omega)$ in another way. Indeed,

$$|f| = \sum_{t=0}^{M-1} f(t)|t\rangle = \sum_{\omega=0}^{M-1} \left( \sum_{t=0}^{M-1} F(\omega) \exp(2\pi t\omega/M) \right)|t\rangle = \sum_{\omega=0}^{M-1} F(\omega) \left( \sum_{t=0}^{M-1} \exp(2\pi t\omega/M)|t\rangle \right) = \sum_{\omega=0}^{M-1} F(\omega)|\omega\rangle,$$

where $|\omega\rangle := \sum_{t=0}^{M-1} \exp(2\pi t\omega/M)|t\rangle = \mathcal{F}_M|t\rangle$. This means that in order to apply the Fourier transformation on general state $|f\rangle$, is sufficient to apply the following transformation on the classical states: $|\omega\rangle = \mathcal{F}_M|t\rangle$.

The classical Cooley–Tukey FFT factorization for $(m^n \times m^n)$–DFT is given by:

$$\mathcal{F}_{m^n} = P_{m^n} \prod_{i=1}^{n} \left[ I_{m^{n-i}} \odot \prod_{k=1}^{n-i} \left( I_{m^{k-1}} \otimes D(\varepsilon^{m^{n-i-k-1}}) \otimes I_{m^{n-i-k-1}} \right) \right] \left[ I_{m^{i-1}} \otimes \mathcal{F}_m \otimes I_{m^{n-i}} \right],$$

(18)

where $P_{m^n}$ is MIT–Reversal permutation matrix, $\varepsilon = e^{2\pi i/m^n}$ denotes a primitive $m^n$th root of unity, and $D(\varepsilon^{m^{n-i-k-1}}) := \text{diag}(1, \varepsilon, \varepsilon^{m^{-1}}, \ldots, \varepsilon^{(m-1)m^{-i-k-1}})$ are diagonal matrices of twiddle factors. If we use direct order for “time mits” and reverse order for “frequency mits” $t = (t_1, t_2, \ldots, t_n) = t_1 m^{n-1} + t_2 m^{n-2} + \ldots + t_n m^0$, $\omega = (\omega_1, \ldots, \omega_2, \omega_1) = \omega_1 m^{n-1} + \ldots + \omega_2 m^1 + \omega_1 m^0$, then we can omit MIT–Reversal permutation matrix in (18).

According to (14) and (15)

$$\left[ I_{m^{i-1}} \otimes \mathcal{F}_m \otimes I_{m^{n-i}} \right] = \mathcal{F}^{(i)}_{m^n}, \quad \left[ I_{m^{i-1}} \otimes \prod_{k=1}^{n-i} \left( I_{m^{k-1}} \otimes D(\varepsilon^{m^{n-i-k-1}}) \otimes I_{m^{n-i-k-1}} \right) \right] = D_{m,k}^{-1}.$$

Therefore, for quantum Fourier transform we have $\mathcal{Q}\mathcal{F}_{m^n} := \prod_{i=1}^{n} \left[ \prod_{k=1}^{n-i} D_{m,k}^{-1} \right] \mathcal{F}^{(i)}$. In the language of quantum circuits, this transform is presented in Fig. 5.

As we showed above, a signal (time–frequency–phase distribution) $f(t, \omega, c): \mathcal{H}\mathcal{W}_{2n+1}(p^n, p^n, p^n) \rightarrow \mathbb{C}$ defined on the Heisenberg group has $p^{2n}$ scalar–valued and $p - 1 (p^n \times p^n)$–matrix–valued spectral components:

$$F(\alpha_1, \alpha_2) = \sum_{t \in GF^n} \sum_{\omega \in GF^n} \sum_{c \in GF^n} f(t, \omega, c) e_p(\alpha_1, t) e_p(\alpha_2, \omega), \quad \tilde{F}_{p^n \times p^n}(\alpha_3) = \sum_{t \in GF^n} \sum_{\omega \in GF^n} \sum_{c \in GF^n} f(t, \omega, c) S^t D(\alpha_3, \omega, c),$$

where $\alpha_1, \alpha_2 \in GF^n(p), \alpha_3 \in GF(p)$. In order to realize quantum Fourier Heisenberg–Weyl transform, we introduce

- input composite quantum register (see Fig. 6) $QU–p^{2n+1}\text{InREG}$ consisting of three quantum registers:

  - $QU–p^{n}\text{REG}(|t\rangle) := |t_1\rangle |t_2\rangle \cdots |t_n\rangle$ is the “time” quantum register,

  - $QU–p^{n}\text{REG}(|\omega\rangle) := |\omega_1\rangle |\omega_2\rangle \cdots |\omega_n\rangle$ is the “frequency” quantum register,

  - $QU–p^1\text{REG}(|c\rangle) := |t_1\rangle$ is the one pit “phase” quantum register and
From expression of the classical fast Fourier–Heisenberg–Weyl transform
\[
FHW = \left[ I_p^{\omega_n-2n} \otimes (I_p^n \otimes F_p^n) \right] \left[ I_p \otimes F_p^n \otimes I_p^n \right] \left[ I_p \otimes F_p^n \otimes I_p^n \otimes I_p^n \right]
\]
we obtain the following quantum fast Fourier–Heisenberg–Weyl transform:
\[
\mathcal{QFHW} = \left[ \prod_{j_\omega=1}^{n} I_p^{\omega n-j_\omega} \otimes F_{p}^{\omega n-j_\omega} \otimes I_p^{n-j_\omega} \right] \left[ I_p \otimes \prod_{i_t=1}^{n} F_{p}^{(i_t)} \otimes I_p^n \right] \left[ F_{p}^{(1c)} \right]
\]
where
\[
\prod_{j_\omega=1}^{n} I_p^{\omega n-j_\omega} \otimes F_{p}^{\omega n-j_\omega} := I_p^{3n-2n} \otimes (I_p^n \otimes F_p^n), \quad I_p \otimes \prod_{i_t=1}^{n} F_{p}^{(i_t)} \otimes I_p^n := I_p \otimes F_p^n \otimes I_p^n,
\]
\[
F_{p}^{(1c)} := \left[ F_p \otimes I_p^n \otimes I_p^n \right].
\]
In the language of quantum circuits, this transform is presented in Fig. 6. From the factorization (19) and quantum circuits structure (14)–(16), we see that the quantum FHW transformation can be implemented by using \( n + 1 \) local gates and \( n + 1 \) \( \omega \)-controlled gates. In fact, the discussed quantum implementation FHWT by using (19) will result in complexity of \( \mathcal{O}(2n + 1) \) by using \( \mathcal{O}(2n + 1) \) gates.

4. ACKNOWLEDGEMENT

This research was performed at the Signal Processing Laboratory, Tampere University of Technology, Finland. The work was also supported by Ural State Technical University, Ekaterinburg, Russia.
REFERENCES

13. R.S. Stancovic, C. Morago, J. Astola, Readings in Fourier Analysis on Finite non–Abelian groups, TICSP Series, 5, TUT, Tampere, 1999
19. V.V. Vedral, A. Barenco and A. Ekert, “Quantum networks for elementary arithmetic operations”. Physical Review A, 54, pp. 147–153,