Block components of generalized quaternion group codes

Nadja Willenborg[1]

[1]University of St.Gallen, Switzerland

Abstract

Codes in the generalized quaternion group algebra $\mathbb{F}_q[Q_{4n}]$ are considered. Restricting to $\mathrm{char}\mathbb{F}_q \nmid 4n$ the structure of an arbitrary code $C \subseteq \mathbb{F}_q[Q_{4n}]$ is described via the Wedderburn decomposition. Moreover it is known that in this case every code $C \subseteq \mathbb{F}_q[Q_{4n}]$ has a generating idempotent $\lambda \in \mathbb{F}_q[Q_{4n}]$. Given the generating idempotent of a code C we determine the different components in its decomposition $C \cong \bigoplus_{j=1}^{r+s} C_j \oplus \bigoplus_{i=1}^{k+t} C_i'$. Afterwards we apply this result to describe the blocks of codes induced by cyclic group codes.

1 Introduction

The primary motivation of this chapter is rooted in physics where the theory of motion control and analysis are related to quaternion groups. It is also known that lattices in quaternion algebras yield space-time codes that achieve high spectral efficiency on wireless channels with two transmit antennas, see [1]. For an overview on proposed post-quantum cryptosystems and digital signature schemes, see for example [4], for applications in quantum computation [7]. Understanding these applications serves the desire to dive into structured areas of noncommutative groups, to finally get generic group algebra cyclotomically, see [3] for more details. In fact, this perspective allows us to identify and understand the block decomposition of codes $C \subseteq \mathbb{F}_q[Q_{4n}]$ which is required when transforming these codes to lifted product codes as done in [10].

Informally, the generalized quaternion group Q_{4n}[1] of order $4n$ considered in [5] is generated by a rotation x by an angle of $\frac{2\pi}{n}$, an arbitrary reflection y and defining relations

$$x^{2n} = 1, y^2 = x^n, yxy^{-1} = x^{-1}.$$

Throughout, let the characteristic of $\mathbb{F}_q$ be coprime to $4n$. In this case every vector space $C \subseteq \mathbb{F}_q[Q_{4n}]$ has a generating idempotent, i.e., an element $\lambda \in \mathbb{F}_q[Q_{4n}]$ such that $\lambda^2 = \lambda$, see [8]. It is known from [6, 8] that for a monic polynomial $f \in \mathbb{F}_q[x]/(x^{2n}-1)$ which divides $x^{2n}-1$, the generating idempotent of the ideal $(f(x))\mathbb{F}_q[x]/(x^{2n}-1)$ is

$$e_g(x) = -\frac{[(g(x)^*)']^*}{2n} \cdot \frac{x^{2n}-1}{g(x)}, \tag{1.1}$$

where $g(x) = \frac{x^{2n}-1}{f(x)}$. Moreover it is shown in [8] that for $g \in \mathbb{F}_q[x]/(x^{2n}-1)$, a monic divisor of $x^{2n}-1$ with $g = g_1 \cdot g_2$, it holds

$$e_g(x) = e_{g_1}(x) + e_{g_2}(x). \tag{1.2}$$

[1]The cyclic group of order $2n$ is a commutative normal subgroup of Q_{4n} of index 2, and so Q_{4n} is solvable.

Recall that an idempotent is said to be irreducible, if it cannot be decomposed into a sum of several nonzero idempotents. Moreover an idempotent is said to be central if it belongs to the center of $\mathbb{F}_q[Q_{4n}]$.

For any monic polynomial $g \in \mathbb{F}_q[x]$ with $g(0) = a_0$, the reciprocal polynomial is defined as $g^*(x) = a_0^{-1}x^{\deg(g)}g(x^{-1})$. We say that g is selfreciprocal if $g = g^*$. In particular g and g^* have the same roots in its splitting field.

Suppose that $x^n - 1$ and $x^n + 1 \in \mathbb{F}_q[x]$ split into monic irreducible factors as follows:

$$x^n - 1 = f_1(x)f_2(x)\cdots f_r(x)f_{r+1}(x)f^*_{r+1}(x)\cdots f_{r+s}(x)f^*_{r+s}(x),$$
$$x^n + 1 = g_1(x)g_2(x)\cdots g_t(x)g_{t+1}(x)g^*_{t+1}(x)\cdots g_{t+k}(x)g^*_{t+k}(x),$$

where $f_j(x) = f^*_j(x)$ for $1 \le j \le r$ and $g_i(x) = g^*_i(x)$ for $1 \le i \le t$. Moreover, $f_1(x) = x - 1, f_2(x) = x + 1$ if n is even; and $f_1(x) = x - 1, g_1(x) = x + 1$ if n is odd. Here α_j denotes a root of f_j and β_i denotes a root of g_i. We set

$$\delta(n) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 2 & \text{if } n \text{ is even,} \end{cases} \quad \mu(n) = \begin{cases} 1 & \text{if } n \text{ is odd,} \\ 0 & \text{if } n \text{ is even.} \end{cases}$$

Moreover we define

$$F_j := \begin{cases} \mathbb{F}_q & 1 \le j \le \delta(n), \\ \mathbb{F}_q[\alpha_j + \alpha_j^{-1}] & \delta(n) + 1 \le j \le r, \\ \mathbb{F}_q[\alpha_j] & r + 1 \le j \le r + s, \end{cases} \quad L_i := \begin{cases} \mathbb{F}_q & 1 \le i \le \mu(n), \\ \mathbb{F}_q[\beta_i + \beta_i^{-1}] & \mu(n) + 1 \le i \le t, \\ \mathbb{F}_q[\beta_i] & t + 1 \le i \le t + k, \end{cases}$$

and

$$I_j(x,y) := \begin{cases} \{ax, by : a, b \in \mathbb{F}_q\} & 1 \le j \le \delta(n), \\ \left\{ \begin{pmatrix} ay & -ax \\ by & -bx \end{pmatrix} : a, b \in F_j \right\} & \delta(n) + 1 \le j \le r + s, \end{cases}$$

$$J_i(x,y) := \begin{cases} \{ax, by : a, b \in \mathbb{F}_q\} & 1 \le i \le \mu(n), \\ \left\{ \begin{pmatrix} ay & -ax \\ by & -bx \end{pmatrix} : a, b \in L_i \right\} & \mu(n) + 1 \le i \le t + k. \end{cases}$$

Note that $I_1(1,0) = \mathbb{F}_q \oplus 0, I_1(0,1) = 0 \oplus \mathbb{F}_q$. Thus for $1 \le j \le \delta(n)$ it suffices to consider $I_j(0,1)$ and $I_j(1,0)$. Similar observations are useful for $1 \le i \le \mu(n)$. For $\delta(n) + 1 \le j \le r + s, \mu(n) + 1 \le i \le k + t$ we consider $I_j(0,1)$ and $I_j(q_j,1)$, respectively $J_i(0,1), J_i(q_i,1)$ where $q_j \in F_j$, respectively $q_i \in L_i$.

By Maschke's theorem the group algebra $\mathbb{F}_q[Q_{4n}]$ is semisimple and hence isomorphic to a direct sum of matrix algebras over suitable extension fields, realized in [5] by the map ρ,

$$\rho : \mathbb{F}_q[Q_{4n}] \to \left(\bigoplus_{j=1}^{r+s} A_j \right) \oplus \left(\bigoplus_{i=1}^{t+k} B_i \right),$$

which is defined by families of $\mathbb{F}_q$-algebra homomorphisms $(\tau_j)_{1 \le j \le r+s}$, $(\eta_i)_{1 \le i \le k+t}$ such that

$$A_j = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q & j \le \delta(n), \\ \mathrm{Mat}_2(\mathbb{F}_q[\alpha_j + \alpha_j^{-1}]) & \delta(n) + 1 \le j \le r, \\ \mathrm{Mat}_2(\mathbb{F}_q[\alpha_j]) & r + 1 \le j \le r + s, \end{cases}$$

$$B_i = \begin{cases} \mathbb{F}_q \oplus \mathbb{F}_q & i \leq \mu(n), \\ \mathrm{Mat}_2(\mathbb{F}_q[\beta_i + \beta_i^{-1}]) & \mu(n)+1 \leq i \leq t, \\ \mathrm{Mat}_2(\mathbb{F}_q[\beta_i]) & t+1 \leq i \leq t+k. \end{cases}$$

As in [9] one can observe that the inverse ρ^{-1} is well-defined and each direct summand $(A_j)_{1\leq j\leq r+s}$, $(B_i)_{1\leq i\leq t+k}$ has an identity element id_{A_j}, respectively id_{B_i}, such that the central irreducible idempotents $(e_j)_{1\leq j\leq r+s}, (e'_i)_{1\leq i\leq t+k}$ are given by

$$e_j = \rho^{-1}(0,\ldots,0,\mathrm{id}_{A_j},0,\ldots,0),\ 1 \leq j \leq r+s, \tag{1.3}$$

$$e'_i = \rho^{-1}(0,\ldots,0,\mathrm{id}_{B_i},0,\ldots,0),\ 1 \leq i \leq k+t. \tag{1.4}$$

Moreover, similarly as in [8], the structure of an arbitrary code $C \subseteq \mathbb{F}_q[Q_{4n}]$ can be described via the decomposition $C \cong \bigoplus_{j=1}^{r+s} C_j \oplus \bigoplus_{i=1}^{t+k} C'_i$, where

$$C_j = \begin{cases} A_j & j \in S_1, \\ I_j(-q_j,1) & j \in S_2 \setminus \{1,\delta(n)\}, \\ I_j(0,1) & j \in S_2 \cap \{1,\delta(n)\}, \\ I_j(1,0) & j \in S_3, \\ 0 & j \notin S_1 \cup S_2 \cup S_3, \end{cases} \quad C'_i = \begin{cases} B_i & i \in S_4, \\ J_i(-q'_i,1) & i \in S_5 \setminus \{1,\mu(n)\}, \\ J_i(0,1) & i \in S_5 \cap \{1,\mu(n)\}, \\ J_i(1,0) & i \in S_6, \\ 0 & i \notin S_4 \cup S_5 \cup S_6, \end{cases}$$

$S_1, S_2, S_3 \subseteq [r+s], S_4, S_5, S_6 \subseteq [k+t]$ are pairwise disjoint and $(q_j)_{j\in S_2} \subseteq F_j$, $(q'_i)_{i\in S_5} \subseteq L_i$.

2 Main result

Theorem 2.1. Let $\gcd(4n,q)=1$ and consider an arbitrary code $C \subseteq \mathbb{F}_q[Q_{4n}]$ generated by its idempotent $\lambda \in \mathbb{F}_q[Q_{4n}]$. Suppose that

$$\phi_j = \lambda e_{f_j}(x),\ 1 \leq j \leq r+s, \qquad \tilde{\phi}_j = \lambda e_{f_j^*}(x),\ r+1 \leq j \leq r+s,$$
$$\psi_i = \lambda e_{g_i}(x),\ 1 \leq i \leq k+t, \qquad \tilde{\psi}_i = \lambda e_{g_i^*}(x),\ t+1 \leq i \leq k+t,$$

and let $\rho(C) = \bigoplus_{j=1}^{r+s} C_i \oplus \bigoplus_{i=1}^{k+t} C'_i$ be the code decomposition. Then the code blocks $(C_j)_{1\leq j\leq r+s}, (C'_i)_{1\leq i\leq t+k}$ are determined by the elements $\phi_j, \tilde{\phi}_j, \psi_i, \tilde{\psi}_i, 1 \leq j \leq r+s, 1 \leq i \leq t+k$ as follows:

(i) For $1 \leq j \leq \delta(n)$

$$C_j = \begin{cases} I_j(1,0) & \text{if } \phi_j = \frac{1+y}{2} e_{f_j}(x), \\ I_j(0,1) & \text{if } \phi_j = \frac{1-y}{2} e_{f_j}(x), \\ 0 & \text{if } \phi_j = 0, \\ A_j & \text{if } \phi_j = e_{f_j}(x). \end{cases}$$

(ii) For $\delta(n)+1 \leq j \leq r$

$$C_j = \begin{cases} 0 & \text{if } \phi_j = 0, \\ A_j & \text{if } \phi_j = e_{f_j}(x). \end{cases}$$

(iii) For $r+1 \leq j \leq r+s$ and $u_j, \tilde{u_j}, v_j, \tilde{v_j} \in \mathbb{F}_q[x]$ such that

$$\phi_j = u_j(x) + y v_j(x), \quad \tilde{\phi}_j = \tilde{u_j}(x) + y\tilde{v_j}(x),$$

we have

$$C_j = \begin{cases} I_j(\tilde{v_j}(\alpha_j^{-1}), -u_j(\alpha_j)) & \text{if } (\tilde{v_j}(\alpha_j^{-1}), u_j(\alpha_j)) \neq (0,0), \\ I_j(\tilde{u_j}(\alpha_j^{-1}), -v_j(\alpha_j)) & \text{if } \tilde{v_j}(\alpha_j^{-1}) = u_j(\alpha_j) = 0 \wedge (\tilde{u_j}(\alpha_j^{-1}), v_j(\alpha_j)) \neq (0,0), \\ 0 & \text{if } \tilde{u_j}(\alpha_j^{-1}) = v_j(\alpha_j) = \tilde{v_j}(\alpha_j^{-1}) = u_j(\alpha_j) = 0, \\ A_j & \text{if } \tilde{v_j} = v_j = 0 \wedge u_j(x) = e_{f_j}(x) \wedge \tilde{u_j}(x) = e_{f_j}(x). \end{cases}$$

(iv) For $1 \leq i \leq \mu(n)$ and $q \equiv 1 \pmod 4$

$$C_i' = \begin{cases} J_i(1,0) & \text{if } \psi_i = -\left(\frac{e_{g_i}(x) - \sqrt{-1}y}{2}\right), \\ J_i(0,1) & \text{if } \psi_i = -\left(\frac{e_{g_i}(x) + \sqrt{-1}y}{2}\right), \\ 0 & \text{if } \psi_i = 0, \\ B_i & \text{if } \psi_i = -e_{g_i}(x). \end{cases}$$

For $1 \leq i \leq \mu(n)$ and $q \equiv 3 \pmod 4$

$$C_i' = \begin{cases} 0 & \text{if } \psi_i = 0, \\ B_i & \text{if } \psi_i = -e_{g_i}(x). \end{cases}$$

(v) For $\mu(n) + 1 \leq i \leq t$

$$C_i' = \begin{cases} 0 & \text{if } \psi_i = 0, \\ B_i & \text{if } \psi_i = -e_{g_i}(x). \end{cases}$$

(vi) For $t+1 \leq i \leq t+k$ and $u_i, \tilde{u_i}, v_i, \tilde{v_i} \in \mathbb{F}_q[x]$ such that

$$\psi_i = u_i(x) + yv_i(x), \quad \tilde{\psi_i} = \tilde{u_i}(x) + y\tilde{v_i}(x),$$

we have

$$C_i' = \begin{cases} J_i(\tilde{v_i}(\beta_i^{-1}), -u_i(\beta_i)) & \text{if } (\tilde{v_i}(\beta_i^{-1}), u_i(\beta_i)) \neq (0,0), \\ J_i(\tilde{u_i}(\beta_i^{-1}), -v_i(\beta_i)) & \text{if } \tilde{v_i}(\beta_i^{-1}) = u_i(\beta_i) = 0 \wedge (\tilde{u_i}(\beta_i^{-1}), v_i(\beta_i)) \neq (0,0), \\ 0 & \text{if } \tilde{u_i}(\beta_i^{-1}) = v_i(\beta_i) = \tilde{v_i}(\beta_i^{-1}) = u_i(\beta_i) = 0, \\ B_i & \text{if } \tilde{v_i} = v_i = 0 \wedge u_i(x) = e_{g_i}(x) \wedge \tilde{u_i}(x) = e_{g_i}(x). \end{cases}$$

Proof. Let δ_{ij} be the Kronecker delta, i.e., $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ if $i \neq j$. Using the central irreducible idempotents obtained in [5], Theorem 3.2 and Theorem 3.8, together with (1.3) and (1.4) we have

$$\sum_{j=1}^{r} e_{f_j} + \sum_{j=r+1}^{r+s} (e_{f_j} + e_{f_j^*}) - \sum_{i=1}^{t} e_{g_i} - \sum_{i=t+1}^{t+k} (e_{g_i} + e_{g_i^*}) = 1.$$

Let

$$\rho(\lambda) = \bigoplus_{j=1}^{r+s} \lambda_j \oplus \bigoplus_{i=1}^{t+k} \lambda_i', \quad \lambda_j \in A_j, \lambda_i' \in B_i,$$

giving for $1 \leq j \leq r$

$$\rho(\phi_j) = \bigoplus_{i=1}^{r+s} \lambda_j \delta_{ij}$$

and for $r+1 \leq j \leq r+s$

$$\rho(\phi_j + \tilde{\phi_j}) = \bigoplus_{i=1}^{r+s} \lambda_j \delta_{ij}.$$

Similarly for $1 \leq i \leq t$

$$\rho(\psi_i) = \bigoplus_{j=1}^{t+k} \lambda'_i \delta_{ij}$$

and for $t+1 \leq i \leq t+k$

$$\rho(\psi_i + \tilde{\psi_i}) = \bigoplus_{j=1}^{t+k} \lambda'_i \delta_{ij}.$$

Thus the elements $(\lambda_j)_{1\leq j\leq r+s}, (\lambda'_i)_{1\leq i\leq t+k}$ can be calculated from $\phi_j, \tilde{\phi_j}, \psi_i, \tilde{\psi_i}$. It follows from

$$\rho(C) = \rho(\mathbb{F}_q[Q_{4n}]\lambda) = \bigoplus_{j=1}^{r+s} A_j\lambda_j \oplus \bigoplus_{i=1}^{t+k} B_i\lambda'_i$$

that $C_j = A_j\lambda_j$, respectively $C'_i = B_i\lambda'_i$.

Cases $(i), (ii), (iv)$ and (v) can easily be deduced from

$$\rho(\phi_j) = \bigoplus_{j=1}^{r+s} \lambda_j \delta_{ij}, \quad \rho(\psi_i) = \bigoplus_{i=1}^{t+k} \lambda'_i \delta_{ij},$$

and Theorem 3.2, Theorem 3.8 from [5] where the central irreducible idempotents covering the possible values of $(\phi_j)_{1\leq j\leq r}, (\psi_i)_{1\leq i\leq t}$ are explicitly given. We exemplarily give arguments proving case (vi) which works similar as case (iii) If

$$\psi_i = u_i(x) + yv_i(x), \quad \tilde{\psi_i} = \tilde{u_i}(x) + y\tilde{v_i}(x),$$

then

$$\lambda'_i \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} u_i(\beta_i) & 0 \\ v_i(\beta_i) & 0 \end{pmatrix}, \quad \lambda'_i \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & \tilde{v_i}(\beta_i) \\ 0 & \tilde{u_i}(\beta_i) \end{pmatrix},$$

and hence

$$\lambda'_i = \begin{pmatrix} u_i(\beta_i) & \tilde{v_i}(\beta_i^{-1}) \\ v_i(\beta_i) & \tilde{u_i}(\beta_i^{-1}) \end{pmatrix}.$$

Obviously, if $\psi_i = \tilde{\psi_i} = 0$, then $\lambda'_i = 0$ and hence $C'_i = 0$. If $\psi_i = e_{g_i}(x)$ and $\tilde{\psi_i} = e_{g_i^*}(x)$, then $\lambda'_i = I_2$ and $C'_i = B_i$.

Moreover, since λ'_i is an idempotent by defintion, it follows from the linear independence of the rows of the matrix λ'_i that $\lambda'_i = I_2$. Therefore, if $\psi_i \neq 0, \tilde{\psi_i} \neq 0, \psi_i \neq e_{g_i}(x), \tilde{\psi_i} \neq e_{g_i^*}(x)$, we have

$$C'_i = \begin{cases} J_i(\tilde{v_i}(\beta_i^{-1}), -u_i(\beta_i)) & \text{if } (\tilde{v_i}(\beta_i^{-1}), u_i(\beta_i)) \neq (0,0), \\ J_i(\tilde{u_i}(\beta_i^{-1}), -v_i(\beta_i)) & \text{if } (\tilde{u_i}(\beta_i^{-1}), v_i(\beta_i)) \neq (0,0), \\ 0 & \text{if } (\tilde{v_i}(\beta_i^{-1}), u_i(\beta_i)) = (\tilde{u_i}(\beta_i^{-1}), v_i(\beta_i)) = (0,0). \end{cases}$$

□

Remark 2.2. For $r+1 \leq j \leq r+s$ with $C_j = A_j$ we require $\phi_j = e_{f_j}(x), \tilde{\phi_j} = e_{\tilde{f}_j}(x)$. Similarly, for $t+1 \leq i \leq t+k$ with $C'_i = B_i$ we require $\psi_i = e_{g_i}(x), \tilde{\psi_i} = e_{\tilde{g}_i}(x)$.

3 Application to induced codes

In the following we apply Theorem 2.1 to obtain the structure of codes induced by cyclic groups. Let ℓ be a positive integer divisor of $2n$. Consider the cyclic group algebra $\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}}-1)$ and let

$$\hat{x}^{\frac{2n}{\ell}}-1=\left(\prod_{j=1}^{\hat{r}}\hat{f}_j(\hat{x})\right)\left(\prod_{j=\hat{r}+1}^{\hat{r}+\hat{s}}\hat{f}_j(\hat{x})\hat{f}_j^*(\hat{x})\right)\left(\prod_{i=1}^{\hat{t}}\hat{g}_i(\hat{x})\right)\left(\prod_{i=\hat{t}+1}^{\hat{t}+\hat{k}}\hat{g}_i(\hat{x})\hat{g}_i^*(\hat{x})\right)$$

be the factorization of $\hat{x}^{\frac{2n}{\ell}}-1$ into irreducible factors. Let

$$\Omega:\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}}-1)\hookrightarrow\mathbb{F}_q[Q_{4n}],\hat{x}\mapsto x^\ell$$

be the embedding of $\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}}-1)$ into $\mathbb{F}_q[Q_{4n}]$. In analogy with (1.1) one can define the idempotent $\hat{e}_h(\hat{x})$ for a monic polynomial $h\in\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}}-1)$ which divides $\hat{x}^{\frac{2n}{\ell}}-1$. Moreover, using (1.2), it is easy to see that if h is irreducible one can write

$$\hat{e}_h(x^\ell)=\left(\sum_{\substack{j=1\\ f_j(x)|h(x^\ell)}}^{r+s}e_{f_j}(x)\right)+\left(\sum_{\substack{j=r+1\\ f_j^*(x)|h(x^\ell)}}^{r+s}e_{f_j^*}(x)\right)+\left(\sum_{\substack{i=1\\ g_i(x)|h(x^\ell)}}^{k+t}e_{g_i}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i^*(x)|h(x^\ell)}}^{k+t}e_{g_i^*}(x)\right)$$

The following observations on generating idempotents immediately follow

Lemma 3.1. Let $(\hat{f}_j)_{1\le j\le r+s},(\hat{f}_j^*)_{r+1\le j\le r+s},(\hat{g}_i)_{1\le i\le t+k}$ and $(\hat{g}_i^*)_{t+1\le i\le t+k}$ be the irreducible factors of $\hat{x}^{\frac{2n}{\ell}}-1$ in $\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}}-1)$.

- For $1\le j\le\hat{r}$

$$\hat{e}_{\hat{f}_j}(x^\ell)=\left(\sum_{\substack{i=1\\ f_i(x)|\hat{f}_j(x^\ell)}}^{r}e_{f_i}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i(x)|\hat{f}_j(x^\ell)}}^{r+s}(e_{f_i}(x)+e_{f_i^*}(x))\right)$$
$$+\left(\sum_{\substack{i=1\\ g_i(x)|\hat{f}_j(x^\ell)}}^{t}e_{g_i}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i(x)|\hat{f}_j(x^\ell)}}^{t+k}(e_{g_i}(x)+e_{g_i^*}(x))\right).$$

- For $\hat{r}+1\le j\le\hat{r}+\hat{s}$

$$\hat{e}_{\hat{f}_j}(x^\ell)=\left(\sum_{\substack{i=r+1\\ f_i(x)|\hat{f}_j(x^\ell)}}^{r+s}e_{f_i}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i^*(x)|\hat{f}_j(x^\ell)}}^{r+s}e_{f_i^*}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i(x)|\hat{f}_j(x^\ell)}}^{t+k}e_{g_i}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i^*(x)|\hat{f}_j(x^\ell)}}^{t+k}e_{g_i^*}(x)\right),$$
$$\hat{e}_{\hat{f}_j^*}(x^\ell)=\left(\sum_{\substack{i=r+1\\ f_i(x)|\hat{f}_j(x^\ell)}}^{r+s}e_{f_i^*}(x)\right)+\left(\sum_{\substack{i=r+1\\ f_i^*(x)|\hat{f}_j(x^\ell)}}^{r+s}e_{f_i}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i(x)|\hat{f}_j(x^\ell)}}^{t+k}e_{g_i^*}(x)\right)+\left(\sum_{\substack{i=t+1\\ g_i^*(x)|\hat{f}_j(x^\ell)}}^{t+k}e_{g_i}(x)\right).$$

- For $1 \leq i \leq \hat{t}$

$$\hat{e}_{\hat{g}_i}(x^\ell) = \left(\sum_{\substack{j=1 \\ f_j(x)|\hat{g}_i(x^\ell)}}^{r} e_{f_j}(x) \right) + \left(\sum_{\substack{j=r+1 \\ f_j(x)|\hat{g}_i(x^\ell)}}^{r+s} (e_{f_j}(x) + e_{f_j^*}(x)) \right) + \left(\sum_{\substack{j=1 \\ g_j(x)|\hat{g}_i(x^\ell)}}^{t} e_{g_j}(x) \right) + \left(\sum_{\substack{j=t+1 \\ g_j(x)|\hat{g}_i(x^\ell)}}^{t+k} (e_{g_j}(x) + e_{g_j^*}(x)) \right).$$

- For $\hat{t}+1 \leq i \leq \hat{t}+\hat{k}$

$$\hat{e}_{\hat{g}_i}(x^\ell) = \left(\sum_{\substack{j=r+1 \\ f_j(x)|\hat{g}_i(x^\ell)}}^{r+s} e_{f_j}(x) \right) + \left(\sum_{\substack{j=r+1 \\ f_j^*(x)|\hat{g}_i(x^\ell)}}^{r+s} e_{f_j^*}(x) \right) + \left(\sum_{\substack{j=t+1 \\ g_j(x)|\hat{g}_i(x^\ell)}}^{t+k} e_{g_j}(x) \right) + \left(\sum_{\substack{i=t+1 \\ g_j^*(x)|\hat{g}_i(x^\ell)}}^{t+k} e_{g_j^*}(x) \right),$$

$$\hat{e}_{\hat{g}_i^*}(x^\ell) = \left(\sum_{\substack{j=r+1 \\ f_j(x)|\hat{g}_i^*(x^\ell)}}^{r+s} e_{f_j^*}(x) \right) + \left(\sum_{\substack{j=r+1 \\ f_j^*(x)|\hat{g}_i^*(x^\ell)}}^{r+s} e_{f_j}(x) \right) + \left(\sum_{\substack{j=t+1 \\ g_j(x)|\hat{g}_i^*(x^\ell)}}^{t+k} e_{g_j^*}(x) \right) + \left(\sum_{\substack{j=t+1 \\ g_j^*(x)|\hat{g}_i^*(x^\ell)}}^{t+k} e_{g_j}(x) \right).$$

Theorem 3.2. Set $\hat{C}_h = (h)$ and let $C = \mathbb{F}_q[Q_{4n}]\Omega(\hat{C}_h)$ be the code induced by $\hat{C}_h$. Then C decomposes as

$$C \cong \bigoplus_{j=1}^{r+s} C_j \oplus \bigoplus_{i=1}^{t+k} C_i',$$

where

$$C_j = \begin{cases} A_j & j \in S_1, \\ I_j(0,1) & j \in S_2, \\ I_j(1,0) & j \in S_3, \\ 0 & j \notin S_1 \cup S_2 \cup S_3, \end{cases} \qquad C_i' = \begin{cases} B_i & i \in S_4, \\ J_i(0,1) & i \in S_5, \\ J_i(1,0) & i \in S_6, \\ 0 & i \notin S_4 \cup S_5 \cup S_6, \end{cases}$$

and

$$\begin{aligned} S_1 &= \{j \in \{1,\ldots,r+s\} : f_j(x) \nmid h(x^\ell) \wedge f_j^*(x) \nmid h(x^\ell)\}, \\ S_2 &= \{j \in \{\delta(n)+1,\ldots,r+s\} : f_j(x) \nmid h(x^\ell) \wedge f_j^*(x) \mid h(x^\ell)\}, \\ S_3 &= \{j \in \{\delta(n)+1,\ldots,r+s\} : f_j(x) \mid h(x^\ell) \wedge f_j^*(x) \nmid h(x^\ell)\}, \\ S_4 &= \{i \in \{1,\ldots,k+t\} : g_i(x) \nmid h(x^\ell) \wedge g_i^*(x) \nmid h(x^\ell)\}, \\ S_5 &= \{i \in \{\mu(n)+1,\ldots,k+t\} : g_i(x) \nmid h(x^\ell) \wedge g_i^*(x) \mid h(x^\ell)\}, \\ S_6 &= \{i \in \{\mu(n)+1,\ldots,k+t\} : g_i(x) \mid h(x^\ell) \wedge g_i^*(x) \nmid h(x^\ell)\}. \end{aligned}$$

Proof. Recalling the generating idempotent $e_g(x)$ given in (1.1) and that for $g \in \mathbb{F}_q[x]/(x^{2n}-1)$, a monic divisor of $x^{2n}-1$ with $g = g_1 \cdot g_2$, it holds $e_g(x) = e_{g_1}(x) + e_{g_2}(x)$, the generating idempotent of the code $\hat{C}_h$ has the form:

$$\hat{e}_{\hat{C}_h}(\hat{x}) = \left(\sum_{\substack{j=1 \\ \hat{f}_j(\hat{x}) \nmid h(\hat{x})}}^{r+s} \hat{e}_{\hat{f}_j}(\hat{x}) \right) + \left(\sum_{\substack{j=1 \\ \hat{f}_j^*(\hat{x}) \nmid h(\hat{x})}}^{r+s} \hat{e}_{\hat{f}_j^*}(\hat{x}) \right) + \left(\sum_{\substack{i=1 \\ \hat{g}_i(\hat{x}) \nmid h(\hat{x})}}^{t+k} \hat{e}_{\hat{g}_i}(\hat{x}) \right) + \left(\sum_{\substack{i=1 \\ \hat{g}_i^*(\hat{x}) \nmid h(\hat{x})}}^{t+k} \hat{e}_{\hat{g}_i^*}(\hat{x}) \right).$$

This gives:

$$C = \mathbb{F}_q[Q_{4n}]\Omega(\hat{C}_h) = \mathbb{F}_q[Q_{4n}]\Omega\left(\mathbb{F}_q[\hat{x}]/(\hat{x}^{\frac{2n}{\ell}} - 1)e_{\hat{C}_h}(\hat{x})\right) = \mathbb{F}_q[Q_{4n}]e_{\hat{C}_h}(x^\ell)$$

and from Lemma 3.1 we have

$$\hat{e}_{\hat{C}_h}(x^\ell) = \left(\sum_{\substack{j=1 \\ f_j(x)\nmid h(x^\ell)}}^{r+s} e_{f_j}(x)\right) + \left(\sum_{\substack{j=r+1 \\ f_j^*(x)\nmid h(x^\ell)}}^{r+s} e_{f_j^*}(x)\right) + \left(\sum_{\substack{i=1 \\ g_i(x)\nmid h(x^\ell)}}^{t+k} e_{g_i}(x)\right) + \left(\sum_{\substack{i=t+1 \\ g_i^*(x)\nmid h(x^\ell)}}^{t+k} e_{g_i^*}(x)\right).$$

Applying Theorem 2.1 the statement follows. □

4 Conclusion

The block components $(C_j)_{1\leq j\leq r+s}, (C'_i)_{1\leq i\leq t+k}$ of a code $C \subseteq \mathbb{F}_q[Q_{4n}]$ with decomposition $C \cong \bigoplus_{j=1}^{r+s} C_j \oplus \bigoplus_{i=1}^{k+t} C'_i$ were identified via its generating idempotent. Afterwards this result is applied to establish the structure of codes induced by cyclic groups. Understanding the structure and decomposition of such induced codes is a key step for the construction of lifted product codes as demonstrated in [10]. Similarly as one can determine the blocks of codes induced by cyclic group codes one can also obtain the blocks of codes in $\mathbb{F}_q[Q_{4n}]$ induced by dihedral group codes, see [10]. However this case requires a rigourous computation of the generating idempotent of dihedral codes, see [8], resulting in a more detailed analysis, see [5, 2]. As already demonstrated in [9] where the bases, the generating and the check matrices of the dihedral codes are constructed one can use the algebra homomorphisms $(\tau_j)_{1\leq j\leq r+s}, (\eta_i)_{1\leq i\leq t+k}$ explicitly given in [5], to extend this to the generalized quaternion group algebra $\mathbb{F}_q[Q_{4n}]$.

Acknowledgements

This work is part of my PhD thesis under the supervision of Anna-Lena Horlemann. I would like to thank Anna-Lena Horlemann for her valuable guidance, constant encouragement to work on group codes and for helpful comments on my work.

References

[1] Grégory Berhuy and Frédérique Oggier, *An introduction to central simple algebras and their applications to wireless communication*, vol. 191, American Mathematical Soc., 2013.

[2] Fabio Enrique Brochero Martínez, Lilian Batista de Oliveira, and Carmen Rosa Giraldo Vergara, *Wedderburn decomposition and idempotents of some finite metacyclic group algebras*, arXiv e-prints (2022), arXiv–2210.

[3] Maria Chlouveraki, *Blocks and families for cyclotomic hecke algebras*, no. 1981, Springer Science & Business Media, 2009.

[4] Steven D Galbraith and Frederik Vercauteren, *Computational problems in supersingular elliptic curve isogenies*, Quantum Information Processing **17** (2018), no. 10, 265.

[5] Yanyan Gao and Qin Yue, *Idempotents of generalized quaternion group algebras and their applications*, Discrete Mathematics **344** (2021), no. 5, 112342.

[6] Fabio Enrique Brochero Martínez, *Structure of finite dihedral group algebra*, Finite Fields and Their Applications **35** (2015), 204–214.

[7] Ori Parzanchevski and Peter Sarnak, *Super-golden-gates for pu(2)*, Advances in Mathematics **327** (2018), 869–901.

[8] Kirill Vladimirovich Vedenev and Vladimir Mikhailovich Deundyak, *Relationship between codes and idempotents in a dihedral group algebra*, Mathematical Notes **107** (2020), no. 1, 201–216.

[9] ———, *The codes in some non–semisimple dihedral group algebras and their properties*, arXiv preprint arXiv:2005.08283 (2020).

[10] Nadja Willenborg, Martino Borello, Anna-Lena Horlemann, and Habibul Islam, *Dihedral quantum codes*, arXiv preprint arXiv:2310.15092 (2023).