Proceedings of the Edinburgh Mathematical Society (2019) **62**, 641–654
doi:10.1017/S0013091518000500

UNITARY AND SYMMETRIC UNITS OF A COMMUTATIVE GROUP ALGEBRA

V. A. BOVDI[1*] AND A. N. GRISHKOV[2]

[1] *UAEU, Al-Ain, United Arab Emirates* (vbovdi@gmail.com)
[2] *IME USP, Citade Universitària, Sao Paulo, Brazil* (shuragri@gmail.com)
and
Omsk F.M. Dostoevsky State University, Omsk Russia

(Received 29 January 2017; first published online 27 December 2018)

Abstract Let F be a field of characteristic two and G a finite abelian 2-group with an involutory automorphism η. If $G = H \times D$ with non-trivial subgroups H and D of G such that η inverts the elements of H (H without a direct factor of order 2) and fixes D element-wise, then the linear extension of η to the group algebra FG is called a *nice involution*. This determines the groups of unitary and symmetric normalized units of FG. We calculate the orders and the invariants of these subgroups.

Keywords: group ring; unitary group; symmetric element; commutative ring; involution

2010 *Mathematics subject classification:* Primary 16S34; 16U60
Secondary 20C05

1. Introduction

Let F be a field with two elements, and G a finite abelian 2-group with an automorphism η of order 2. Extending η to the group algebra FG by setting

$$\left(\sum_{g\in G}\alpha_g g\right)^{\eta} = \sum_{g\in G}\alpha_g g^{\eta}$$

we obtain an involution of the algebra FG (which will be called η as well). In the group

$$V(FG) = \left\{\sum_{g\in G}\alpha_g g \in FG \mid \sum_{g\in G}\alpha_g = 1\right\}$$

of (normalized) units of FG, the subgroups of η-unitary units and of η-symmetric units are defined, respectively, by

$$V_\eta(FG) = \{x \in V(FG) \mid x^{\eta} = x^{-1}\} \quad \text{and} \quad S_\eta(FG) = \{x \in V(FG) \mid x^{\eta} = x\}.$$

* Corresponding author.

© 2018 The Edinburgh Mathematical Society

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

We intend to study these groups for a certain type of involution. We call η a *nice involution* provided that

$$G = H \times D$$

with subgroups H and D of G such that η inverts the elements of H and fixes D element-wise. We then always assume that H has no direct factor of order 2.

When η is the canonical involution $*$ (i.e. the linear extension of the anti-automorphism $g \mapsto g^{-1}$ of G to the group algebra KG), the problem of determining the invariants and an explicit basis of $V_*(FG)$ has been raised by Novikov (see [**15**]). A satisfactory solution for $*$ was given in [**8**, **10**]; these results were extended later in [**11**] to abelian p-groups of odd order. In this paper, we calculate the orders and invariants of the two groups $S_\eta(FG)$ and $V_\eta(FG)$ for the 2-group G when η is a nice involution. The determination of explicit bases remains open. However, we give an explicit description of the group of unitary units.

Theorem 1.1. *Let η be a nice involution of a finite abelian 2-group G. Then the group of η-unitary units in the normalized group of units $V(FG)$ of the group algebra FG over the field F of characteristic 2 is given by*

$$V_\eta(FG) = H \cdot (W(FG) \times \Omega V(FD) \times T(G))$$

and

$$\log |V_\eta(FG)| = \log |\Omega H| + \tfrac{1}{2}(|G| + |\Omega H||D|) - |D^2|.$$

Here, $W(FG) = \{x^\eta x^{-1} \mid x \in V(FG)\}$, which is obviously a subgroup of $V_\eta(FG)$. The group $T(G)$ is an elementary abelian subgroup of $V_\eta(FG)$, to be defined later in § 4, and is related to Sandling's multiplicative basis of $V(FG)$ (see [**16**]). For a positive integer i, we shall write $\Omega_i G$ for the subgroup of G of all elements of order dividing 2^i (and abbreviate Ω_1 to Ω). The logarithm is to base 2, of course.

Much of the following depends on the observation that the 2nd power mapping $\varphi : x \mapsto x^2$ is an F-algebra endomorphism of FG.

We remark that commutative modular group algebras have several applications in coding theory [**1**, **2**, **18**], cryptography [**13**, **14**], bent function theory [**6**] and threshold logic [**3**]. For a non-commutative group algebra, the study of unitary and symmetric units is an interesting problem by itself, with many applications (see [**4**, **5**, **7**, **9**, **12**, **17**]).

2. η-symmetric units

First, we indicate how to calculate the invariants of $S_\eta(FG)$.

We begin with some preparations for our first lemma, so as not to obstruct the view of the line of proof. We suppose that η is a nice involution. We write G_η for the subgroup of fixed points of η on G. Obviously, we can choose a subset E of $G \setminus G_\eta$ such that $E \cap E^\eta = \varnothing$ and $G = G_\eta \cup E \cup E^\eta$ (disjoint union). Since η acts on the cosets of G_η in G, we can even choose E as a union of cosets of G_η in G. We set $E_0 = \{e \in E \mid e^2 \in G_\eta\}$ and $E_1 = E \setminus E_0$, so that $E = E_0 \cup E_1$ (disjoint union). Note that if $e \in E_0$, we can write $e = hd$ with $h \in H$, $d \in D$ and h of order 4, since $e \notin G_\eta$ but $e^2 \in G_\eta$, and then $hD \subseteq E_0$. Also, if h is an element of H of order 4, then either h or h^{-1} belongs to E_0 (since the

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

action of η interchanges both elements). Remembering that $|\Omega_2 P| = |\Omega P| \cdot |\Omega P^2|$ for any abelian 2-group P, we therefore have

$$|E_0| = \tfrac{1}{2}(|\Omega_2 H| - |\Omega H|) \cdot |D| = \tfrac{1}{2}|\Omega H| \cdot (|\Omega H^2| - 1) \cdot |D|. \tag{2.1}$$

Let $X = \Omega G \subseteq G_\eta$. We also note that $E_0 X \subseteq EX \subseteq E$ and $(E_0 X)^2 = E_0^2 \subseteq G_\eta$, so $E_0 X = E_0$ and $E_1 X = E_1$.

We have $G_\eta = \Omega H \times D$. So $|E| = 1/2(|G| - |G_\eta|) = 1/2(|G| - |\Omega H| \cdot |D|)$. Taking this together with (2.1) it follows that

$$|E_1| = |E| - |E_0| = \tfrac{1}{2}(|G| - |\Omega H| \cdot |\Omega H^2| \cdot |D|).$$

We have $|X| = |\Omega H||\Omega D|$. Remembering that for any abelian 2-group P, we have $|P| \setminus |\Omega P| = |P^2|$, we finally obtain what will be needed in our first lemma

$$\frac{|E_1|}{|X|} = \frac{1}{2}(|G^2| - |\Omega H^2||D^2|). \tag{2.2}$$

Lemma 2.1. *Suppose that η is a nice involution. Then the following hold:*

(i) $\log |S_\eta(FG)| = 1/2(|G| + |\Omega H||D|) - 1$;

(ii) $\log |S_\eta(FG)^2| = 1/2(|G^2| - |\Omega H^2||D^2|) + |D^2| - 1$.

Proof. Each $x \in S_\eta(FG)$ can be written as

$$x = \sum_{e \in E} \alpha_e (e + e^\eta) + \sum_{g \in G_\eta} \beta_g g \tag{2.3}$$

with uniquely determined coefficients α_e (for $e \in E$) and β_g (for $g \in G_\eta$) in F such that $\sum_{g \in G_\eta} \beta_g = 1$. Conversely, given such coefficients from F, Equation (2.3) defines an element x from $S_\eta(FG)$. Hence

$$\begin{aligned}\log |S_\eta(FG)| &= |E| + |G_\eta| - 1 \\ &= \tfrac{1}{2}(|G| - |G_\eta|) + |G_\eta| - 1 = \tfrac{1}{2}(|G| + |G_\eta|) - 1.\end{aligned}$$

Now $G_\eta = \Omega H \times D$ and (i) follows.

Squaring both sides of (2.3) gives

$$x^2 = \sum_{e \in E} \alpha_e (e^2 + (e^2)^\eta) + \sum_{g \in G_\eta} \beta_g g^2. \tag{2.4}$$

Let T be a system of coset representatives of X in G_η. Then we can write for the second summand on the right-hand side of (2.4)

$$\sum_{g \in G_\eta} \beta_g g^2 = \sum_{t \in T} \sum_{x \in X} \beta_{tx} (tx)^2 = \sum_{t \in T} \left(\sum_{x \in X} \beta_{tx} \right) t^2.$$

Note that $s^2 \neq t^2$ for $s, t \in T$ with $s \neq t$. We have $|T| = |\Omega H \times D| / |\Omega H \times \Omega D| = |D^2|$. The first summand on the right-hand side of (2.4) really extends over only the elements

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

e from E_1. Since $E_1X = E_1$, we can choose $S \subseteq E_1$ such that E_1 is the disjoint union of the cosets sX, $s \in S$. Then we have

$$\begin{aligned}\sum_{e\in E_1} \alpha_e(e^2 + (e^2)^\eta) &= \sum_{s\in S}\sum_{x\in X} \alpha_{sx}((sx)^2 + ((sx)^2)^\eta)\\ &= \sum_{s\in S}\biggl(\sum_{x\in X}\alpha_{sx}\biggr)(s^2 + (s^2)^\eta).\end{aligned}$$

Again, note that $s^2 \neq t^2$ for $s, t \in S$ with $s \neq t$.

We have seen that the number of 'free parameters' for a unit in $S_\eta(FG)^2$ is $|S| + |D^2| - 1$. From (2.2), which gives us $|S|$, (ii) follows. □

3. The unit group modulo η-symmetric units

Suppose that η is a nice involution; explicitly, $G = H \times D$ such that the automorphism η is given by $h^\eta = h^{-1}$ for $h \in H$ and $d^\eta = d$ for $d \in D$, where H has no direct factor of order 2.

We denote by $C_n^{(m)}$ a direct product of m copies of a cyclic group of order $n > 1$. Then, for some positive integers k and integers $m_1, \ldots, m_k \geq 0$ (multiplicities), we have

$$H \cong C_{2^{k+1}}^{(m_k)} \times \cdots \times C_8^{(m_2)} \times C_4^{(m_1)}.$$

We set $H_0 = H$ and $D_0 = D$, so $G = G^{2^0} = H_0 \times D_0$. Note that η induces an automorphism on each 2-power of G. For $i \geq 0$, there are (essentially) unique subgroups H_i and D_i of G^{2^i} with $G^{2^i} = H_i \times D_i$ and H_i having no direct factor of order 2, such that $h^\eta = h^{-1}$ for $h \in H_i$ and $d^\eta = d$ for $d \in D_i$. For $0 \leq i < k$, an easy induction on i (we set $m_0 = 0$) shows that

$$G^{2^i} \cong \underbrace{C_{2^{k-(i-1)}}^{(m_k)} \times \cdots \times C_4^{(m_{i+1})}}_{\cong H_i} \times \underbrace{C_2^{(m_i)} \times D^{2^i}}_{\cong D_i}.$$

(For the induction step, notice that when we take the second power of G^{2^i}, the factor $C_2^{(m_i)}$ vanishes.) For example, we have

$$G^{2^{k-1}} \cong \underbrace{C_4^{(m_k)}}_{\cong H_{k-1}} \times \underbrace{C_2^{(m_{k-1})} \times D^{2^{k-1}}}_{\cong D_{k-1}}.$$

Furthermore, $G^{2^k} = D_k \cong C_2^{(m_k)} \times D^{2^k}$ and $G^{2^i} = D^{2^i}$ for $i > k$.

Now observe that for $i \geq 0$,

$$\log|\Omega H_i| = \sum_{j=i+1}^{k} m_j \quad \text{and} \quad \log|\Omega H^{2^i}| = \sum_{j=i}^{k} m_j$$

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

(with the usual convention for the empty sum). For $i \geq 0$, it follows that

$$\begin{aligned}\log(|\Omega H_i| \cdot |D_i|) &= \log|\Omega H_i| + \log|D_i| \\ &= \left(\sum_{j=i+1}^{k} m_j\right) + (m_i + \log|D^{2^i}|) \\ &= \left(\sum_{j=i}^{k} m_j\right) + \log|D^{2^i}| \quad \text{(shift it back)} \\ &= \log|\Omega H^{2^i}| + \log|D^{2^i}| = \log(|\Omega H^{2^i}||D^{2^i}|),\end{aligned}$$

that is,

$$|\Omega H_i||D_i| = |\Omega H^{2^i}||D^{2^i}| \quad \text{for } i \geq 0. \tag{3.1}$$

Lemma 2.1(i), applied to G^{2^i} instead of G, shows that for $i \geq 0$ we have

$$\log|S_\eta(FG^{2^i})| = \tfrac{1}{2}(|G^{2^i}| + |\Omega H_i||D_i|) - 1.$$

Taking this together with (3.1), we obtain

$$\log|S_\eta(FG^{2^i})| = \tfrac{1}{2}(|G^{2^i}| + |\Omega H^{2^i}||D^{2^i}|) - 1 \quad \text{for } i \geq 0. \tag{3.2}$$

We dispose of a homomorphism $\psi : V(FG) \to V_\eta(FG)$, given by $\psi(x) = x^\eta x^{-1}$ for $x \in V(FG)$. By definition, the kernel of ψ is $S_\eta(FG)$. The image of ψ will be denoted by $W(FG)$. So, $W(FG) = \{x^\eta x^{-1} \mid x \in V(FG)\}$, and we have an exact sequence

$$1 \longrightarrow S_\eta(FG) \longrightarrow V(FG) \longrightarrow W(FG) \longrightarrow 1. \tag{3.3}$$

We only remark that this sequence, when defined for odd p, is split.

Lemma 3.1. *The following hold.*

(i) $W(FG^{2^i}) = W(FG)^{2^i}$ *and*

$$\log|W(FG^{2^i})| = \tfrac{1}{2}(|G^{2^i}| - |\Omega H^{2^i}||D^{2^i}|) \quad \textit{for all } i \geq 0.$$

(ii) $\log|\Omega W(FG)| = \frac{1}{2}(|G| - |\Omega H||D|) - \frac{1}{2}(|G^2| - |\Omega H^2||D^2|)$.

Proof. Inclusion $W(FG)^2 \subseteq W(FG^2)$ is straightforward. If $x \in V(FG)$, then writing $x = \sum_{g\in G} \alpha_g g$ shows that $x^2 = \sum_{g\in G} \alpha_g g^2 \in V(FG^2)$ and so

$$(x^\eta x^{-1})^2 = (x^2)^\eta (x^2)^{-1} \in W(FG^2).$$

The same argument shows that each element of $V(FG^2)$ is the square of an element of $V(FG)$. An element x in $V(FG^2)$ can be written as $\sum_{g\in G} \alpha_g g^2$ for some choice of coefficients, and setting $y = \sum_{g\in G} \alpha_g g$ we have $y \in V(FG)$ and $y^2 = x$. It follows that

$$x^\eta x^{-1} = (y^\eta y^{-1})^2 \in W(FG)^2,$$

showing that $W(FG^2) \subseteq W(FG)^2$. Hence $W(FG^2) = W(FG)^2$, and induction shows that $W(FG^{2^i}) = W(FG)^{2^i}$ for all $i \geq 0$.

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

From (3.3), applied to G^{2^i} instead of G, and (3.2), we obtain

$$\begin{aligned}\log|W(FG^{2^i})| &= \log|V(FG^{2^i})| - \log|S_\eta(FG^{2^i})| \\ &= (|G^{2^i}|-1) - (\tfrac{1}{2}(|G^{2^i}| + |\Omega H^{2^i}||D^{2^i}|) - 1) \\ &= \tfrac{1}{2}(|G^{2^i}| - |\Omega H^{2^i}||D^{2^i}|),\end{aligned}$$

completing the proof of (i).

Finally, (ii) follows from (i) since $|P| = |P/P^2|$ for any abelian 2-group P. □

Obviously, $S_\eta(FG)^{2^i} \leq S_\eta(FG^{2^i})$, but equality cannot be expected here. Indeed, by (3.2) and Lemma 2.1(ii), we have

$$\log|S_\eta(FG^2) : S_\eta(FG)^2| = (|\Omega H^2| - 1)|D^2|.$$

4. Elementary abelian subgroups

We suppose that η is a nice involution, that is, we have $G = H \times D$ with subgroups H and D of G such that η inverts the elements of H and fixes D element-wise, and we assume that H has no direct factor of order 2. We can write $H = H_1 \times \cdots \times H_r$ with (non-trivial) cyclic subgroups H_i of H. Let $\mathcal{P}$ denote the power set of $\{1, \ldots, r\}$ minus the singleton $\{\varnothing\}$. For $\mathcal{S} \in \mathcal{P}$, let $H_{\mathcal{S}} = \langle H_i \mid i \in \mathcal{S}\rangle \leq G$, and let $\widehat{H_{\mathcal{S}}}$ denote the sum of the elements of $H_{\mathcal{S}}$ in FG.

We define, on the basis of these choices, the set

$$T(G) = \left\{1 + \sum_{\mathcal{S}\in\mathcal{P}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}} \mid c_{\mathcal{S}} \in FD \quad \text{for all } \mathcal{S} \in \mathcal{P}\right\}.$$

Applying the Frobenius endomorphism to the elements of $T(G)$, we see that its elements $\neq 1$ are units of order 2, since $(\widehat{H_{\mathcal{S}}})^2 = 0$ for $\mathcal{S} \in \mathcal{P}$. Obviously, $T(G)$ is closed under multiplication, so $T(G)$ is an elementary abelian subgroup of $V(FG)$.

We will count the number of elements in $T(G)$. Suppose that there is a relation $\sum_{\mathcal{S}\in\mathcal{P}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}} = c$, with $c \in FD$ and also all $c_{\mathcal{S}}$ in FD. We claim that c and all $c_{\mathcal{S}}$ are 0. We proceed by induction on r, the base case $r = 1$ being obvious. Let $r > 1$. We can rewrite the relation as

$$\widehat{H_{\{1\}}} \sum_{\mathcal{S}\in\mathcal{P},\, 1\in\mathcal{S}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}\setminus\{1\}}} + \sum_{\mathcal{S}\in\mathcal{P},\, 1\notin\mathcal{S}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}} = c$$

(with the convention that $\widehat{H_\varnothing} = 1$). Here, both sums on the left-hand side have support in the subgroup $U = (H_2 \times \cdots \times H_r)D$. Picking a generator h_1 of H_1 and comparing coefficients of elements of the coset h_1U on both sides of the relation shows that the first sum is 0. By the induction hypothesis, our claim follows. Note that $|\mathcal{P}| = 2^r - 1$. Thus,

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

we have shown that $|T(G)| = |FD|^{|\mathcal{P}|} = 2^{|D|}(2^r - 1)$. With $2^r = |\Omega H|$ we obtain

$$\log|T(G)| = (|\Omega H| - 1)|D|. \tag{4.1}$$

For later use, we note that

$$B = \{1 + d\widehat{H_{\mathcal{S}}} \mid \mathcal{S} \in \mathcal{P}, d \in D\}$$

is a minimal generating set of $T(G)$. In fact, it has the right cardinality. If $\mathcal{S} \in \mathcal{P}$ and $c = \sum_{d \in D} \alpha_d D \in FD$, all $\alpha_d \in F$, then

$$1 + c\widehat{H_{\mathcal{S}}} = \prod_{d \in D} (1 + \alpha_d d\widehat{H_{\mathcal{S}}}) \in \langle B \rangle.$$

Suppose that $c_{\mathcal{S}} \in FD$ (for $\mathcal{S} \in \mathcal{P}$) are such that $\prod_{\mathcal{S} \in \mathcal{P}}(1 + c_{\mathcal{S}}\widehat{H_{\mathcal{S}}}) = 1$, with some $c_{\mathcal{S}} \neq 0$. Choose M in $\mathcal{P}$ of minimal cardinality with $c_M \neq 0$. Multiplying out, we obtain

$$0 = \prod_{\mathcal{S} \in \mathcal{P}} (1 + c_{\mathcal{S}}\widehat{H_{\mathcal{S}}}) - 1 = \sum_{\mathcal{S} \in \mathcal{P}} c'_{\mathcal{S}}\widehat{H_{\mathcal{S}}}$$

for some $c'_{\mathcal{S}} \in FD$, and obviously $c'_M = c_M \neq 0$, in contradiction to the above-noted additive independence of the elements $\widehat{H_{\mathcal{S}}}$. Hence, multiplicative independence follows from additive independence (the connection with Sandling's multiplicative basis for $V(FG)$ should be clear at this time).

We have to define, for G^2, the group $T(G^2)$ in a compatible way. We may suppose that $H_1, \ldots, H_s$, for some s, are the factors of H of order > 4. Then $A = H_{s+1} \times \cdots \times H_r$ is a direct product of cyclic groups of order 4 (possibly $A = 1$). Let $\mathcal{P}'$ denote the power set of $\{1, \ldots, s\}$ minus $\{\varnothing\}$. We have

$$G^2 = (H_1^2 \times \cdots \times H_s^2) \times (A^2 \times D^2)$$

where the factors on the right-hand side are the 'new H' and the 'new D'. So we define

$$T(G^2) = \left\{1 + \sum_{\mathcal{S} \in \mathcal{P}'} c_{\mathcal{S}}\widehat{H^2_{\mathcal{S}}} \;\middle|\; c_{\mathcal{S}} \in F[A^2 \times D^2] \quad \text{for all } \mathcal{S} \in P'\right\}.$$

We now clarify the position of $T(G)$ relative to some other subgroups of $V(FG)$.

Lemma 4.1. *The following hold.*

(i) $T(G) \cap W(FG) = 1$.

(ii) *The group Q generated by $\Omega V(FD)$, $T(G)$ and $W(FG)$ is a direct product,*

$$Q = W(FG) \times \Omega V(FD) \times T(G).$$

Proof. Let $x \in T(G) \cap W(FG)$. We will prove $x = 1$ by induction on the order of G. We can write $x = 1 + \sum_{\mathcal{S} \in \mathcal{P}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}}$ with uniquely determined $c_{\mathcal{S}}$ in FD. Fix some i between 1 and r and set $K_i = \langle H_j | 1 \leq j \leq r, j \neq i\rangle$. We have a natural isomorphism

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

$G/H_i \cong K_i \times D$ which we shall treat as an identification. Let bars denote the natural map $FG \to FG/H_i$. Note that η induces on the abelian group $\overline{G}$ a nice involution, with associated decomposition $\overline{G} = K_i \times D$. Also $\overline{T(G)} = T(F\overline{G})$ if $T(F\overline{G})$ is properly defined, and obviously $\overline{W(FG)} \subseteq W(F\overline{G})$. Hence we can assume inductively that $\overline{x} = 1$, which means $\sum_{\mathcal{S}\in\mathcal{P},\, i\notin\mathcal{S}} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}} = 0$. So we have seen that $c_{\mathcal{S}} = 0$ for all $\mathcal{S}$ of cardinality less than r, and we have $x = 1 + c\widehat{H}$ for some $c \in FD$.

Now also $x \in W(FG)$, so $x = y^{-1}y^{\eta}$ for some $y \in V(FG)$. It follows that $y^{-1}y^{\eta} - 1 = c\widehat{H}$ and $y^{\eta} + y = yc\widehat{H} = m\widehat{H}$ for some $m \in FD$. From this we obtain $m = 0$, as otherwise the support of $m\widehat{H}$ would contain an element from D, while the support $y^{\eta} + y$ does not contain an element from D. It follows that $c = 0$ and $x = 1$, proving (i).

Next, note that $\Omega V(FD) \cap T(G) = 1$ simply because $FD \cap T(G) = 1$ (as shown above).

Note that for $y \in T(G)$, we have $y\widehat{H} = \widehat{H}$. Also note that an element of $W(FG)$ is mapped to 1 under the natural map $FG \to FG/H \cong FD$, so for $w \in W(FG)$ we also have $w\widehat{H} = \widehat{H}$. Now suppose that $x \in \Omega V(FD)$ and $y \in T(G)$ are such that $xy \in W(FG)$. Then $\widehat{H} = xy\widehat{H} = x\widehat{H}$, showing that $x = 1$. Now $y = 1$ by (i), and (ii) is proved. □

For later use, we record the following.

Lemma 4.2. *We have* $L(FG) \cap W(FG) = 1$, *where*

$$L(FG) = \left\{ 1 + \sum_{\mathcal{S}\in\mathcal{P}'} c_{\mathcal{S}}\widehat{H_{\mathcal{S}}} \;\middle|\; c_{\mathcal{S}} \in F[A^2 \times D^2] \quad \text{for all } \mathcal{S} \in \mathcal{P}' \right\}.$$

Proof. The proof is the proof of Lemma 4.1(i) with appropriate modifications. □

We need a little preparation before we can compute the orders of the various other groups.

Suppose that K is an arbitrary subgroup of G. We shall write $I(K)$ for the ideal of FK generated by the elements $k - 1$ for $k \in K$ (the radical of FK). Then $I(K)FG$ is the ideal of FG generated by $I(K)$. Note that $FG/I(K)FG$ is naturally isomorphic to $F[G/K]$, the group algebra of the factor group G/K, which gives

$$V(FG)/(1 + I(K)FG) \cong V(F[G/K]).$$

We remark that part (ii) of the following lemma is a special case of Lemma 2.1 from Sandling's paper (see [**16**]). Part (iii) will only be needed once in the proof of Lemma 4.4(i).

Lemma 4.3. *The following hold.*

(i) *Let T be a transversal of K in G. Then a basis over F of the ideal $I(K)FG$ of FG is given by* $\{\, (k-1)t \mid t \in T,\, 1 \neq k \in K\}$.

(ii) $\Omega V(FG) = 1 + I(\Omega G)FG$.

(iii) $\log|\Omega V(FG)| = |G| - |G|^2$.

Proof. Part (i) is well known (and easy to prove).

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

We have $(1 + I(\Omega G)FG)^2 = 1 + I(\Omega G)^2 FG^2 = 1$, showing one inclusion in (ii). Conversely, let $u \in \Omega V(FG)$. Let T denote a transversal of ΩG in G with $1 \in T$, and write $u = \sum_{t\in T} x_t t$ with $x_t \in F\Omega G$ for $t \in T$. Let $\varepsilon(x_t)$ denote the augmentation of x_t. Then

$$1 = \left(\sum_{t\in T} x_t t\right)^2 = \sum_{t\in T} x_t^2 t^2 = \sum_{t\in T} \varepsilon(x_t) t^2,$$

and $s^2 \neq t^2$ for $s, t \in S$ with $s \neq t$, so $\varepsilon(x_1) = 1$ and $\varepsilon(x_t) = 0$ for $1 \neq t \in T$. It follows that $u \in 1 + I(\Omega G)FG$, and (ii) is proved.

We have

$$\begin{aligned}\log|\Omega V(FG)| &= \dim_F I(\Omega G)FG \\ &= (|\Omega G| - 1)\tfrac{|G|}{|\Omega G|} = |G| - |G|^2,\end{aligned}$$

by (ii) and (i), proving (iii). □

Lemma 4.4. *The following hold.*

(i) $\Omega V_\eta(FG) = \Omega W(FG) \times \Omega V(FD) \times T(G)$.

(ii) *For the group* $Q = W(FG) \times \Omega V(FD) \times T(G)$ *from Lemma 4.1(ii), we have* $\log|Q| = \frac{1}{2}(|G| + |\Omega H||D|) - |D^2|$.

(iii) $H \cap Q = H^2 \subseteq W(FG)$.

(iv) $\log|HQ| = \log|\Omega H| + \log|Q|$.

(v) $\log|HQ| - \log|\Omega V_\eta(FG)| = \log|\Omega H| + \frac{1}{2}(|G^2| - |\Omega H^2||D^2|)$.

Proof. First, note that the groups $\Omega V(FD)$, $\Omega W(FG)$ and $T(G)$ are contained in $\Omega V_\eta(FG)$ for obvious reasons, and that their product is direct, by Lemma 4.1. By definition, $\Omega V_\eta(FG) = \Omega S_\eta(FG)$, so we see from Lemma 2.1 that

$$\begin{aligned}\log|\Omega V_\eta(FG)| &= \log|S_\eta(FG)| - \log|S_\eta(FG)^2| \\ &= \tfrac{1}{2}(|G| + |\Omega H||D|) - \tfrac{1}{2}(|G^2| - |\Omega H^2||D^2|) - |D^2|.\end{aligned}$$

By Lemma 3.1(ii), Lemma 4.3(iii) and (4.1), we have

$$\begin{aligned}\log|\Omega W(FG)| &= \tfrac{1}{2}(|G| + |\Omega H||D|) - |\Omega H||D| \\ &\quad - \tfrac{1}{2}(|G^2| - |\Omega H^2||D^2|), \\ \log|\Omega V(FD)| &= |D| - |D^2|, \\ \log|T(G)| &= |\Omega H||D| - |D|.\end{aligned}$$

These ranks add up to the rank of $\Omega V_\eta(FG)$. Thus (i) is proved.

By Lemma 3.1(i), $\log|W(FG)| = 1/2(|G| - |\Omega H||D|)$. Taking this together with the last two displayed equations, (ii) follows.

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

Obviously $H^2 \subseteq W(FG)$ since η inverts the elements of H. So $H^2 \subseteq H \cap Q$. An element of $W(FG)$ can be written as $x^\eta x^{-1}$ for some $x \in V(FG)$. Since η induces the identity on the quotient $F[G/H^2]$, we see that $W(FG)$ maps to 1 under the natural map $FG \to F[G/H^2]$. Also, $T(G)$ is mapped to 1 under this map, since each $\widehat{H_\mathcal{S}}$ is mapped to 0. Now let $h \in H \cap Q$. We have seen that h has the same image in $F[G/H^2]$ as an element of FD. It follows that h maps to 1 under the map $FG \to F[G/H^2]$, so $h \in H^2$, and (iii) is proved.

Finally, (iii) gives

$$|HQ| = |H||Q|/|H \cap Q| = |H||Q|/|H^2| = |\Omega H||Q|,$$

so (iv) holds. Part (v) follows from the above calculations. □

We finally note the following.

Lemma 4.5. *We have $V_\eta(F[A \times D])^2 = A^2$.*

Proof. Suppose that $x \in V_\eta(F[A \times D])$ satisfies $x^2 \neq 1$. Since x^2 lies in the group algebra $F[A^2 \times D]$, on which η acts trivially, x^2 must be an involution and x is of order 4. Let $T \subseteq A \setminus \{1\}$ such that $\{1\} \cap T$ is a transversal of $A^2 \times D$ in $A \times D$. Then T consists of elements of order 4 which are inverted by η. We can write

$$x = \beta_1 + \sum_{t \in T} \beta_t t$$

with $\beta_1, \beta_t \in F[A^2 \times D]$, for all $t \in T$. Then

$$(x^2\beta_1) + \sum_{t \in T}(x^2\beta_t)t = x^2 x = x^{-1} = x^\eta = \beta_1 + \sum_{t \in T}(\beta_t t^2)t.$$

Again, remember that $x^2 \in F[A^2 \times D]$. It follows that $x^2\beta_1 = \beta_1$ and $x^2\beta_t = \beta_t t^2$ for all $t \in T$. The first equation shows that β_1 has augmentation 0 (otherwise β_1 would be a unit and so $x^2 = 1$). Since x has augmentation 1, it follows that some β_t $(t \in T)$ has augmentation 1, whence it is a unit, and therefore $x^2 = t^2 \in A^2$. □

5. A crucial computation

We shall need some kind of 'going up' from $T(G^2)$ to $T(G)$. Suppose that H is a cyclic group of order q, a power of 2, and let h denote a generator of H. We shall write $\widehat{h^i}$ for $\widehat{\langle h^i \rangle}$, for any integer i. We begin by noting the well-known fact that

$$(h+1)^{q-1} = \widehat{H}. \tag{5.1}$$

Indeed, multiplying out $(h+1)^{q-1}$ shows that the element has 1 in its support, so $(h+1)^{q-1} \neq 0$. Also $(h+1)^q = (h^q + 1) = 0$, so $h(h+1)^{q-1} = (h+1)^{q-1}$, giving (5.1).

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

A variation on (5.1) is that

$$(h+1)^{q-2^m} = (h^{2^m}+1)^{q/2^m-1} = \widehat{h^{2^m}}$$

as long as 2^m divides q. For example, if $q \geq 4$, it follows that

$$(h^{\pm 2}+1)^{q-1} = (h^{\pm 2}+1)(h^{\pm 2}+1)^{q-2} = (h^{\pm 2}+1)\widehat{h^4},$$
$$(h^{\pm 1}+1)^{q-3} = (h^{\pm 1}+1)(h^{\pm 1}+1)^{q-4} = (h^{\pm 1}+1)\widehat{h^4}.$$

We will make use of these formulas shortly. We have to introduce some notation only for the formulation and the proof of the next lemma. For a positive $n \in \mathbb{Z}$, let

$$E_n = \{(\varepsilon_1, \ldots, \varepsilon_n) \in \{1, 2, -1\}^n \mid \varepsilon_i \neq 2 \text{ for at least one index } i\}.$$

For $\varepsilon \in E_n$, we shall write $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_n)$, that is, ε_i denotes the ith entry of ε. Let π be the permutation on $\{1, 2, -1\}$ which interchanges 1 and -1. Then an obvious action (component-wise) of the group $\langle \pi \rangle$ of order 2 on E_n is given by $(\varepsilon^\pi)_i = \varepsilon_i^\pi$ $(1 \leq i \leq n)$ for $\varepsilon \in E_n$. Clearly, π acts without fixed points on E_n, so we can choose $E \subset E_n$ with $E_n = E \cup E^\pi$ (disjoint union).

Suppose now that η is a nice involution, and $n \leq r$, so $H_1, \ldots, H_n$ are direct factors of G associated with η on which η acts by inversion. For $1 \leq i \leq n$, let h_i denote a generator of H_i, of order q_i. For $\varepsilon \in E_n$, we define $\nu(\varepsilon) \in \{q_i - 3, q_i - 1\}^n$ as $\nu(\varepsilon) = (\nu(\varepsilon)_i, \ldots, \nu(\varepsilon)_i)$ with $\nu(\varepsilon)_i = q_i - 1$ if $\varepsilon_i = 2$ and $\nu(\varepsilon)_i = q_i - 3$ otherwise. By the formulas above,

$$(h_i^{\varepsilon_i}+1)^{\nu(\varepsilon)_i} = (h_i^{\varepsilon_i}+1)\widehat{h_i^4}$$

for $\varepsilon \in E_n$ and $1 \leq i \leq n$. Finally, we unveil the reason for introducing the set E. We will write $K = H_1 \times \cdots \times H_n$ and let T denote a transversal of K^4 in K^2. Then

$$T + \sum_{\varepsilon \in E_n} \prod_{i=1}^{n} (h_i^{\varepsilon_i}+1)$$

is the sum of the elements of a transversal of K^4 in K, as if we formally multiply out the products in the sum, we obtain a summand $h_{i_1}^{\varepsilon_{i_1}} h_{i_2}^{\varepsilon_{i_2}} \cdots h_{i_l}^{\varepsilon_{i_l}}$, for $1 \leq i_1 < i_2 < \cdots < i_l \leq n$, all $\varepsilon_{i_k} \in \{1, 2, -1\}$ and some ε_{i_k} not $= 2$, exactly 3^{n-l} times.

Lemma 5.1. *With notation as above, suppose that $H_1, \ldots, H_n$ are of order > 4. For a symmetric element c in FG (i.e. $c^\eta = c$), set*

$$u = 1 + c \sum_{\varepsilon \in E_n} \prod_{i=1}^{n} (h_i^{\varepsilon_i}+1)^{\nu(\varepsilon)_i}.$$

Then $u^2 = 1$, and $\psi(u) = u^{-1}u^\eta = (1 + c\widehat{K^2})(1 + c\widehat{K})$, where $K = H_1 \times \cdots \times H_n$.

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

Proof. We calculate

$$\begin{aligned} uu^\eta &= \Big(1 + c \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{\varepsilon_i}+1)^{\nu(\varepsilon)_i}\Big)\Big(1 + c \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{-\varepsilon_i}+1)^{\nu(\varepsilon)_i}\Big)\\ &= \Big(1 + c \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{\varepsilon_i}+1)\widehat{h_i^4}\Big)\Big(1 + c \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{-\varepsilon_i}+1)\widehat{h_i^{-4}}\Big)\\ &= \Big(1 + c\widehat{K^4} \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{\varepsilon_i}+1)\Big)\Big(1 + c\widehat{K^4} \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{-\varepsilon_i}+1)\Big)\\ &= 1 + c\widehat{K^4}\Big(\sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{\varepsilon_i}+1) + \sum_{\varepsilon\in E}\prod_{i=1}^{n}(h_i^{-\varepsilon_i}+1)\Big)\\ &= 1 + c\widehat{K^4}\widehat{T} + c\widehat{K^4}\Big(\widehat{T} + \sum_{\varepsilon\in E_n}\prod_{i=1}^{n}(h_i^{\varepsilon_i}+1)\Big)\\ &= 1 + c(\widehat{K^2}+\widehat{K}) = (1+c\widehat{K^2})(1+c\widehat{K}). \end{aligned}$$

When multiplying out, we used $(\widehat{K^4})^2 = 0$. Note that the first three lines of the calculation show that $u^2 = 1$. □

We shall see that the effort was worthwhile. Recall the definition of $T(G)$ and $T(G^2)$ from the preceding section.

Corollary 5.2. *We have $V_\eta(FG)^2 \cap T(G^2) = \langle 1\rangle$.*

Proof. Suppose that there is $x \in V_\eta(FG)$ such that $1 \neq x^2 \in T(G^2)$. Then x is of order 4 and $x^2 = x^{-1}x^\eta \in W(FG)$. We can write

$$x^2 = \prod_{S\in\mathcal{S}}(1 + c_{\mathcal{S}}\widehat{H^2_{\mathcal{S}}})$$

for some subset S of $\mathcal{P}'$ and non-zero coefficients $c_{\mathcal{S}}$ in $F[A^2 \times D^2]$. By Lemma 5.1,

$$wx^2 = \prod_{S\in\mathcal{S}}(1 + c_{\mathcal{S}}\widehat{H_{\mathcal{S}}}) \in L(FG)$$

for some $w \in W(FG)$. Then $wx^2 = 1$ by Lemma 4.2. But the $1 + c_{\mathcal{S}}\widehat{H_{\mathcal{S}}}$ are multiplicatively independent, so we have reached a contradiction. □

Corollary 5.3. *We have $V_\eta(FG)^2 \cap V(F[A \times D])T(G^2) = A^2$.*

Proof. Set $K = H_1 \times \cdots \times H_s$, so $H = K \times A$ and $G/K \cong A \times D$. Under the natural map $FG \to F[G/K]$, the group $T(G^2)$ maps to 1, while $V(F[A \times D])$ embeds, and

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

$V_\eta(FG)^2$ is mapped into $V_\eta(F[G/K])^2$, which is A^2K/K by Lemma 4.5. It follows that

$$V_\eta(FG)^2 \cap V(F[A \times D])T(G^2) = V_\eta(FG)^2 \cap A^2T(G^2).$$

Since $A^2 \subseteq V_\eta(FG)^2$, we have

$$V_\eta(FG)^2 \cap A^2\,T(G^2) = A^2(V_\eta(FG)^2 \cap T(G^2)).$$

Application of Corollary 5.3 completes the proof. □

6. Proof of the theorem

We finally prove the theorem given in the introduction. The Frobenius endomorphism φ gives rise to an exact sequence

$$1 \longrightarrow \Omega V(FG) \longrightarrow V(FG) \xrightarrow{\varphi} V(FG^2) \longrightarrow 1.$$

Certainly φ commutes with η, so we have an induced exact sequence

$$1 \longrightarrow \Omega V_\eta(FG) \longrightarrow V_\eta(FG) \xrightarrow{\varphi} V_\eta(FG)^2 \longrightarrow 1.$$

The kernel $\Omega V_\eta(FG)$, as well as its order, is known; see Lemma 4.4(i), where the order of HQ, with $Q = W(FG) \times \Omega V(FD) \times T(G)$, is also given. If we can show that for the image

$$\log|V_\eta(FG)^2| = \log|\Omega H| + \tfrac{1}{2}(|G^2| - |\Omega H^2||D^2|) \tag{6.1}$$

holds, we are done by Lemma 4.4(v). Now $V_\eta(FG)^2 \subseteq V_\eta(FG^2)$, and by induction on the order of G, we can assume that $V_\eta(FG^2)$ is described by the theorem. That is,

$$V_\eta(FG^2) = H^2(W(FG^2) \times \Omega V(F[A^2 \times D^2]) \times T(G^2)).$$

We can write $\Omega V(F[A^2 \times D^2]) = A^2 \times M$ for some subgroup M. Then we have $V_\eta(FG)^2 \cap MT(G^2) = 1$ by Corollary 5.3, so

$$V_\eta(FG)^2 \to V_\eta(FG^2)/MT(G^2)$$

is injective. Since $H^2W(FG^2) = H^2W(FG)^2 \subseteq V_\eta(FG)^2$ by Lemma 3.1, it follows that

$$|V_\eta(FG)^2| \le |V_\eta(FG^2)/MT(G^2)| \le |H^2W(FG^2)| \le |V_\eta(FG)^2|.$$

Hence

$$|V_\eta(FG)^2| = |H^2W(FG^2)| = |W(FG^2)||H^2|/|H^2 \cap W(FG^2)|.$$

By part (iii) of Lemma 4.4, applied to the group G^2, we have $H^2 \cap W(FG^2) = H^4$. So

$$|V_\eta(FG)^2| = |W(FG^2)||H^2|/|H^4| = |W(FG^2)||\Omega H|.$$

Finally, by Lemma 3.1(i),

$$\log|W(FG^2)| = \tfrac{1}{2}(|G^2| - |\Omega H^2||D^2|).$$

Thus (6.1) holds and the theorem is proved.

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press

Acknowledgements. We would like to express our deep gratitude to the referee for the thoughtful and constructive review of our manuscript. Comments and remarks of the reviewer considerably influenced the style and the results of our paper.

V.B. was supported by the UAEU UPAR grant: G00002160; A.G. was supported by the Russian Science Foundation (project 16-11-10002) (§§ 1–4), by CNPq (grant 307824/2016-0) and by FAPESP (grant 14/09310-5) (§§ 5–6).

References

1. V. Abdukhalikov, Defining sets of extended cyclic codes invariant under the affine group, *J. Pure Appl. Algebra* **196**(1) (2005), 1–19.
2. V. Abdukhalikov, On codes over rings invariant under affine groups, *Adv. Math. Commun.* **7**(3) (2013), 253–265.
3. N. N. Aĭzenberg, A. A. Bovdi, È. I. Gergo and F. È. Geche, Algebraic aspects of threshold logic (in Russian, with English summary), *Cybernetics* **16**(2) (1980), 188–193.
4. Z. Balogh, L. Creedon and J. Gildea, Involutions and unitary subgroups in group algebras, *Acta Sci. Math. (Szeged)* **79**(3–4) (2013), 391–400.
5. M. Barakat, Computations of unitary groups in characteristic 2, (for J.-P. Serre), preprint, 2013.
6. S. D. Berman and I. I. Grushko, B-functions encountered in modular codes, *Problemy Peredachi Informatsii* **17**(2) (1981), 10–18 (in Russian).
7. V. Bovdi and L. G. Kovács, Unitary units in modular group algebras, *Manuscripta Math.* **84**(1) (1994), 57–72.
8. A. A. Bovdi and A. A. Sakach, The unitary subgroup of the multiplicative group of the modular group algebra of a finite abelian p-group, *Mat. Zametki* **45**(6) (1989), 23–29, 110.
9. V. Bovdi and M. Salim, On the unit group of a commutative ring, *Acta Sci. Math. (Szeged)* **80**(3–4) (2014), 434–445.
10. A. A. Bovdi and A. Szakács, A basis for the unitary subgroup of the group of units in a finite commutative group algebra, *Publ. Math. Debrecen* **46**(1–2) (1995), 97–120.
11. A. Bovdi and A. Szakács, Units of commutative group algebra with involution, *Publ. Math. Debrecen* **69**(3) (2006), 291–296.
12. J. Gildea, The structure of the unitary units of the group algebra $\mathbb{F}_{2^k}D_8$, *Int. Electron. J. Algebra* **9** (2011), 171–176.
13. B. Hurley and T. Hurley, Group ring cryptography, *Int. J. Pure Appl. Math.* **69**(1) (2011), 67–86.
14. B. Hurley and T. Hurley, Paraunitary matrices and group rings, *Int. J. Group Theor.* **3**(1) (2014), 31–56.
15. S. P. Novikov, Algebraic construction and properties of Hermitian analogs of K-theory over rings with involution from the viewpoint of Hamiltonian formalism. Applications to differential topology and the theory of characteristic classes. I. II, *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970), 253–288, 475–500.
16. R. Sandling, Units in the modular group algebra of a finite abelian p-group, *J. Pure Appl. Algebra* **33**(3) (1984), 337–346.
17. J.-P. Serre, Bases normales autoduales et groupes unitaires en caractéristique 2, *Transform. Groups* **19**(2) (2014), 643–698.
18. W. Willems, A note on self-dual group codes, *IEEE Trans. Inform. Theory* **48**(12) (2002), 3107–3109.

https://doi.org/10.1017/S0013091518000500 Published online by Cambridge University Press