Miskolc Mathematical Notes
Vol. 26 (2025), No. 1, pp. 61–67
HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2025.4944

MONTE CARLO METHOD AND GROUP ALGEBRAS

ZSOLT BALOGH

Received 29 January, 2024

Abstract. Let FG be the group algebra of a finite p-group G over a finite field F of characteristic p. Let $\circledast$ be an involution of FG and $V_{\circledast}(FG)$ the $\circledast$-unitary subgroup of FG. The order of $V_{\circledast}(FG)$ is known when p is an odd prime, and $\circledast$ arises from G, however the case of two characteristic is a challenging problem. The RAMEGA package of GAP system contains implementations of functions based on random methods related to group algebras. In this paper we provide the theoretical background of some random functions of RAMEGA that related to the $*$-unitary subgroup of FG, where $*$ is the canonical involution. We estimate the order of the $*$-unitary subgroup of FG for non-abelian 2-groups of order 2^5 using Monte Carlo method. Furthermore, we verify the estimated orders for certain groups of order 2^5.

2010 *Mathematics Subject Classification:* 16S34; 16U60

Keywords: group ring, group of units, unitary subgroup, GAP

1. Introduction

Let FG be the group algebra of a finite p-group G over a finite field F of characteristic p. We denote by $V(FG)$ the normalized unit group of FG, that is,

$$V(FG) = \Big\{ x = \sum_{g\in G} \alpha_g g \in FG \mid \chi(x) = \sum_{g\in G} \alpha_g = 1 \Big\}, \tag{1.1}$$

where $\chi(x)$ is the augmentation map of FG (see [13, Chapters 2-3, p. 194-196]). As a consequence, the order of $V(FG)$ is equal to $|F|^{|G|-1}$ and it is easy to see that $V(FG)$ may be very large even for small group basis G. Therefore, studying the structure of the normalized group of units is a really difficult task. While random methods may serve as effective tools for various purposes, group algebras have yet to be explored using such techniques. Using the formula (1.1) it is easy to obtain a sequence of uniformly distributed random normalized units. In this paper, we propose some random functions and take advantage of them to study the structure of normalized units. The

The research was supported by UAEU Research *Start-up Grant No. G00002968*.

implementations of the functions can be found in our RAMEGA package [3] of the GAP computer algebra system.

While numerous authors have delved into the investigation of the structure of $V(FG)$, our understanding of its structure and that of its subgroups remains limited. For an overview of this topic, we refer the reader to [10] and [13].

Assume $\circledast$ acts as an anti-automorphism on G. This anti-automorphism can be linearly extended to FG, providing an algebra involution of FG which we shall also denote as $\circledast$. In this context, we say that the algebra involution $\circledast$ arises from the group basis G. An example of such an involution arising from G is the canonical $*$-involution, representing the linear extension of the anti-automorphism on G that maps each element of G to its inverse. An element $u \in V(FG)$ is called $\circledast$-*unitary* if $u^{\circledast} = u^{-1}$, with respect to an involution $\circledast$ of FG. The set comprising all unitary elements of $V(FG)$ forms a subgroup denoted as $V_{\circledast}(FG)$ and is referred to as the $\circledast$-unitary subgroup. Interest in the unitary subgroups first appeared in algebraic topology and unitary K-theory, as evidenced by Novikov's paper [19], playing a pivotal role in the examination of the structure of $V(FG)$. For more details we refer the reader to [13]. This subgroup has proven immensely valuable in various studies, as highlighted in [1, 4, 5, 7, 8, 12, 14, 16, 17]. Consider a finite Galois extension L of F with Galois group G, where F is a finite field of characteristic two. Serre, in [20], unveiled an intriguing connection between the self-dual normal basis of L over F and the unitary subgroup of FG. This correlation emphasizes the timeliness and relevance of investigating unitary subgroups.

Although the order the $\circledast$-unitary subgroup of FG, where p is an odd prime and $\circledast$ arises from G is well known [6], the case with characteristic two is a challenging problem. Let $G\{2\}$ be the set of all elements of G having order 2 with the identity. In [11], Bovdi and Sakach gave a formula for the order of the unitary subgroup when G is a finite abelian 2-group, proving that

Proposition 1 (Theorem 2, [11])**.** *Let G be a finite abelian 2-group and F a finite field of characteristic two. Then*

$$|V_*(FG)| = |G^2\{2\}| \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

Computing the order of $V_*(FG)$ remained an open question, when G is a non-abelian 2-group and has been addressed by many authors ever since ([2,9,15,21,22]). In this case it turned out that the order of the $*$-unitary subgroup of FG determines the order of G. Let $\xi(G)$ denote the center of the group G and $\xi(G)\{2\}$ denote the set of elements of order two in $\xi(G)$.

Proposition 2 ([6])**.** *Let G be a finite 2-group. If F is a finite field of characteristic two, then*

$$|V_*(FG)| = \Theta \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$$

for some integer Θ. Moreover, if the set $T_c = \{g \in G \mid g^2 = c\}$ is commutative for some $c \in \xi(G)\{2\}$, then Θ does not depend on the field F.

The parameter Θ has been determined for many groups ([2, 15, 21, 22]), but no general formula has been found for that, except the case when G is an abelian 2-group.

In the next section we present some random methods corresponding to the order of the $*$-unitary subgroup showing their probability theoretical background. These methods together with several others can be found in the RAMEGA package [3] of GAP. With the help of random methods the order of $V_*(FG)$ can be estimated within a reasonable time even for larger group algebras. Using Monte Carlo method we show that Θ can be estimated for all the groups G of order 2^5. We also verify the estimated orders for certain groups of order 2^5.

2. MONTE CARLO METHOD

Let FG be a group algebra of a finite p-group G over a finite field F of characteristic p. Every element of FG can be written as

$$x = \sum_{g \in G} \alpha_g,$$

where $\alpha \in F$. Therefore it is easy to generate a random element from FG with a uniform distribution.

RAMEGA [3] stands for RAndom MEthods in Group Algebras and includes several random methods for studying group algebras. There are also some functions available for the $\circledast$-unitary subgroup, such as *GetRandomNormalizedUnitaryUnit*, *RandomUnitarySubgroup* or *RandomUnitaryOrder*. The function *RandomUnitaryOrder* estimates the order of the $\circledast$-unitary subgroup of FG using Monte Carlo method. For odd primes the function returns the exact value of the order (see Theorem 1 in [6]), however general formula for the order is not known when the group basis G is a non-abelian 2-group. Therefore we deal with only the case when $|F| = 2^m$ for some m and G is a group of order 2^n for some n.

Let us randomly select a unit ξ from the normalized unit group $V(FG)$. The RAMEGA function *GetRandomUnit* can generate a random normalized unit with uniform distribution. Consider the experiment as success if the selected unit is unitary, that is $\xi\xi^* = 1$, otherwise it is failure. To be more precise let ξ be a random variables defined by the following way:

$$\xi = \begin{cases} 1 & \text{if } \xi \text{ is a unitary unit;} \\ 0 & \text{if } \xi \text{ is not a unitary unit.} \end{cases}$$

It is well-known that the distribution of ξ is Bernoulli with parameter q, were $q = \frac{|V_*(FG)|}{|V(FG)|}$. Let us denote by η the distribution of the number k of the Bernoulli trials needed to get one success. The probability $P(\eta = k)$ is equal to $(1-q)^{k-1}q$ therefore η has geometric distribution and its mean $\mu = E(\eta) = \frac{1}{q}$ and its standard deviation is $\sigma = \frac{\sqrt{1-q}}{q}$. Thus $|V_*(FG)|$ can be estimated as $|V_*(FG)| = q \cdot |V(FG)| = \frac{|V(FG)|}{E(\eta)}$.

Since $|G| \leq |V_*(FG)| \leq |V(FG)| = |F|^{|G|-1} = 2^{m|G|-m}$ we conclude that $q = \frac{1}{2^{i_0}}$, where $0 \leq i_0 \leq m|G| - m - n$. The central limit theorem asserts that as the number of replications n increases, the standardized estimator $\frac{\widehat{\mu}-\mu}{\frac{\sigma}{\sqrt{n}}}$ converges in distribution to the standard normal, where $\widehat{\mu} = \frac{\eta_1+\eta_2+\cdots+\eta_n}{n}$, $\mu = \frac{1}{q}$ and $\sigma = \sqrt{\mu(\mu-1)}$. Therefore

$$\lim_{n\to\infty} P\big(|\widehat{\mu}-\mu| \leq \frac{x\sigma}{\sqrt{n}}\big) = \Phi(x).$$

The algorithm works as a statistical test with null hypothesis that the mean $E(\frac{\widehat{\mu}-\mu}{\frac{\sigma}{\sqrt{n}}})$ is zero. The test is at the Z percent confidence level if

$$P(|\widehat{\mu}-\mu| \leq z_p \frac{\sigma}{\sqrt{n}}) = \frac{Z}{100},$$

where $z_p = \Phi^{-1}(\frac{Z}{100})$ and the corresponding confidence interval is $(-z_p \frac{\sigma}{\sqrt{n}}, z_p \frac{\sigma}{\sqrt{n}})$.

Consider n trials such that the ith random sample η_i is x_i. If n is large enough, then $|V_*(FG)|$ can be estimated by $\frac{n\cdot|V(FG)|}{x_1+x_2+\cdots+x_n} = \frac{n\cdot|F|^{|G|-1}}{x_1+x_2+\cdots+x_n}$. Since $|V_*(FG)|$ is a p-group $\frac{n\cdot|F|^{|G|-1}}{x_1+x_2+\cdots+x_n}$ has to be round to the closest power of p.

The pseudocode of our algorithm can be seen in Algorithm 1.

Algorithm 1 Order of unitary subgroup by random way using geometric distribution

```
function RandomUnitaryOrder(kg, n)        ▷ kg is the group algebra, n is the number of trials
    mean ← 0
    trials ← []                           ▷ empty list
    counter ← 0
    grouporder ← order of G
    fieldsize ← size of F
    p ← characteristic of F
    repeat
        m ← 0
        repeat
            x ← random normalized unit
            m ← m + 1
        until x is unitary
        trials ← m;
    until counter = n
    mean = Sum(trials)/Number(trials);
    min ← n(mean − p)^2/p
    position ← 0
    if 1 < mean then
        for i = 1 to LogInt(fieldsize, p) · (grouporder − 1) do
            index ← (n ∗ (mean − p^i)^2)/(p^i ∗ (p^i − 1))
            if index < min then
                min ← index
                position ← i
            end if
        end for
    end if
return fieldsize^(grouporder−1)/p^position
end function
```

Using package RAMEGA we can estimate the order of the $*$-unitary subgroups for the groups of order 2^5 within a reasonable time. For the sake of convenience G_i

represents the group that is returned by the GAP funtion *SmallGroup(2^5,i)* using the library of small groups of GAP [18].

Conjecture 1. *Let G be a non-abelian group of order 2^5 and F is a finite field of characteristic two. Then $|V_*(FG)| = \Theta \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$, where*

(i) $\Theta = 1$ *if* $G \in \{G_{18}, G_{27}, G_{28}, G_{34}, G_{39}, G_{42}, G_{43}, G_{46}, G_{48}, G_{49}, G_{50}\}$;
(ii) $\Theta = 2$ *if*
$$G \in \{G_5, G_6, G_7, G_9, G_{11}, G_{17}, G_{19}, G_{22}, G_{25}, G_{30}, G_{31}, G_{37}, G_{38}, G_{40}, G_{44}\};$$
(iii) $\Theta = 4$ *if*
$$G \in \{G_2, G_4, G_8, G_{10}, G_{12}, G_{13}, G_{14}, G_{15}, G_{20}, G_{23}, G_{24}, G_{29}, G_{33}, G_{41}, G_{47}\};$$
(iii) $\Theta = 8$ *if* $G \in \{G_{26}, G_{32}, G_{35}\}$.

Proposition 3 (Lemma 2.6, [22]). *Let G be a finite group and A an elementary abelian 2-group. If $|V_*(FG)| = \Theta \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$, then*
$$|V_*(F(G \times A))| = \Theta \cdot |F|^{\frac{1}{2}(|G\times A|+|(G\times A)\{2\}|)-1}.$$

Let H be a normal subgroup of G. Let us define S_H to be the set
$$\{xx^* \mid \Psi(x) \in V_*(F\overline{G})\},$$
where $\overline{G} = G/H$ and Ψ is the natural homomorphism from FG to $F\overline{G}$. We will use $\widehat{H}$ to denote the sum of the elements of H in FG.

Theorem 1. *Conjecture 1 is true for the following groups $G_2, G_5, G_{17}, G_{18}, G_{20}, G_{22}, G_{23}, G_{37}, G_{39}, G_{40}, G_{41}, G_{46}, G_{47}, G_{48}$.*

Proof. According to Proposition 3 and Theorem 1.4 in [2]

(i) $\Theta = 1$ if $G \in \{G_{48} \cong D_8 \curlyvee C_4 \times C_2, G_{39} \cong D_{16} \times C_2, G_{46} \cong D_8 \times C_2 \times C_2\}$;
(ii) $\Theta = 2$ if $G \in \{G_{37} \cong M_{16} \times C_2, G_{40} \cong D_{16}^- \times C_2, G_{22} \cong H_{16} \times C_2\}$;
(iii) $\Theta = 4$ if $G \in \{G_{41} \cong Q_{16} \times C_2, G_{23} \cong C_4 \ltimes C_4 \times C_2, G_{47} \cong Q_8 \times C_2 \times C_2\}$.

Let $G = G_2$. Then $G' \cong C_2$, $\overline{G} = G/G' \cong C_4 \times C_4$ and $S_{G'} = \langle\, 1 + \alpha(g + g^{-1})\widehat{G'} \mid \alpha \in F,\ g \in G \setminus G\{2\} \,\rangle$. According to Lemma 1 in [6]
$$|V_*(FG)| = |F|^{|\overline{G}|} \cdot \frac{|V_*(F\overline{G})|}{|S_{G'}|} = |F|^{\frac{1}{2}|G|} \cdot \frac{|V_*(F\overline{G})|}{|F|^{\frac{1}{4}(|G|-|G\{2\}|)}} = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F\overline{G})|.$$

By Theorem 2 in [11] and the fact that $|G\{2\}| = 2|\overline{G}\{2\}|$ we have
$$|V_*(F\overline{G})| = |\overline{G}^2\{2\}| \cdot |F|^{\frac{1}{2}(|\overline{G}|+|\overline{G}\{2\}|)-1} = 4 \cdot |F|^{\frac{1}{2}(|\overline{G}|+|\overline{G}\{2\}|)-1} = 4 \cdot |F|^{\frac{1}{4}(|G|+|G\{2\}|)-1}.$$
Therefore
$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F\overline{G})| = 4 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1},$$

which proves that $\Theta = 4$.

Let $G = G_5$. Then $G' \cong C_2$, $\overline{G} = G/G' \cong C_8 \times C_2$ and $S_{G'} = \langle\, 1 + \alpha(g + g^{-1})\widehat{G'} \mid \alpha \in F,\ g \in G \setminus G\{2\}\,\rangle$. According to Lemma 1 in [6]

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F\overline{G})|.$$

By Theorem 2 in [11] and the fact that $|G\{2\}| = 2|\overline{G}\{2\}|$ we have

$$|V_*(F\overline{G})| = |\overline{G}^2\{2\}| \cdot |F|^{\frac{1}{2}(|\overline{G}|+|\overline{G}\{2\}|)-1} = 2 \cdot |F|^{\frac{1}{2}(|\overline{G}|+|\overline{G}\{2\}|)-1} = 2 \cdot |F|^{\frac{1}{4}|G|+\frac{|G\{2\}|}{4}-1}.$$

Therefore

$$|V_*(FG)| = |F|^{\frac{1}{4}(|G|+|G\{2\}|)} \cdot |V_*(F\overline{G})| = 2 \cdot |F|^{\frac{1}{2}|G|+\frac{|G\{2\}|}{4}+\frac{|G\{2\}|}{4}-1},$$

which proves that $\Theta = 2$.

Let $G = G_{17}$. According to Theorem 1.1 in [5] $|V_*(FG)| = 2 \cdot |F|^{\frac{1}{2}|G|+1}$. Since $|G\{2\}| = 4$ we have $|V_*(FG)| = 2 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}$ so $\Theta = 2$.

Let $G = G_{18} \cong D_{32}$. Then $|G\{2\}| = \frac{|G|}{2} + 2$ and by Corollary 2 in [15]

$$|V_*(FG)| = |F|^{3\frac{|G|}{4}} = |F|^{\frac{|G|}{4}+\frac{|G|}{2}}.$$

Therefore

$$|V_*(FG)| = |F|^{\frac{|G|}{4}-\frac{|G\{2\}|}{2}+1} \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

By Proposition 2 $\Theta = |F|^{\frac{|G|}{4}-\frac{|G\{2\}|}{2}+1} = |F|^{\frac{|G|}{4}-\frac{|G|}{4}-1+1} = 1$.

Let $G = G_{20} \cong Q_{32}$. By Corollary 2 in [15] and the fact that $|G\{2\}| = 2$

$$|V_*(FG)| = 4 \cdot |F|^{\frac{|G|}{2}} = 4 \cdot |F|^{\frac{1}{2}(|G|+|G\{2\}|)-1}.$$

Thereofore $\Theta = 4$ by Proposition 2.

□

ACKNOWLEDGEMENTS

The author would like to thank the anonymous reviewers for their careful reading of the manuscript and their valuable comments and suggestions.

REFERENCES

[1] Z. Balogh, "The structure of the unit group of some group algebras," *Miskolc Mathematical Notes*, vol. 21, no. 2, p. 615, 2020, doi: 10.18514/mmn.2020.3406.

[2] Z. Balogh, "On unitary subgroups of group algebras," *Int. Electron. J. Algebra*, vol. 29, pp. 187–198, 2021, doi: 10.24330/ieja.852199.

[3] Z. Balogh and V. Laver, "RAMEGA – RAndom MEthods in Group Algebras, Version 1.0.0," 2020.

[4] Z. Balogh and V. Laver, "Unitary subgroups of commutative group algebras of characteristic 2," *Ukraïn. Mat. Zh.*, vol. 72, no. 6, pp. 751–757, 2020, doi: 10.37863/umzh.v72i6.1068.

[5] Z. A. Balogh, "Unitary units of the group algebra of modular groups," *Journal of Algebra and Its Applications*, vol. 21, no. 02, nov 2020, doi: 10.1142/s021949882250027x.

[6] Z. A. Balogh, "The order of the unitary subgroups of group algebras," *International Journal of Algebra and Computation*, vol. 32, no. 07, pp. 1327–1334, Jul. 2022, doi: 10.1142/s0218196722500576.

[7] A. Bovdi and L. Erdei, "Unitary units in modular group algebras of groups of order 16," *Technical Reports, Universitas Debrecen, Dept. of Math., L. Kossuth Univ.*, vol. 4, no. 157, pp. 1–16, 1996.

[8] A. Bovdi and L. Erdei, "Unitary units in modular group algebras of 2-groups," *Comm. Algebra*, vol. 28, no. 2, pp. 625–630, 2000, doi: 10.1080/00927870008826848.

[9] A. Bovdi and A. Szakács, "Units of commutative group algebra with involution," *Publ. Math. Debrecen*, vol. 69, no. 3, pp. 291–296, 2006.

[10] A. A. Bovdi, "Unitarity of the multiplicative group of an integral group ring," *Mat. Sb. (N.S.)*, vol. 119(161), no. 3, pp. 387–400, 448, 1982.

[11] A. A. Bovdi and A. A. Sakach, "Unitary subgroup of the multiplicative group of a modular group algebra of a finite abelian p-group," *Mat. Zametki*, vol. 45:6, pp. 23–29, 1989.

[12] 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*, vol. 46, no. 1-2, pp. 97–120, 1995.

[13] A. Bovdi, "The group of units of a group algebra of characteristic p," *Publ. Math. Debrecen*, vol. 52, no. 1-2, pp. 193–244, 1998.

[14] V. Bovdi and L. G. Kovács, "Unitary units in modular group algebras," *Manuscripta Math.*, vol. 84, no. 1, pp. 57–72, 1994, doi: 10.1007/BF02567443.

[15] V. Bovdi and A. L. Rosa, "On the order of the unitary subgroup of a modular group algebra," *Comm. Algebra*, vol. 28, no. 4, pp. 1897–1905, 2000, doi: 10.1080/00927870008826934.

[16] V. Bovdi and M. Salim, "On the unit group of a commutative group ring," *Acta Sci. Math. (Szeged)*, vol. 80, no. 3-4, pp. 433–445, 2014, doi: 10.14232/actasm-013-510-1.

[17] V. A. Bovdi and A. N. Grishkov, "Unitary and symmetric units of a commutative group algebra," *Proc. Edinb. Math. Soc. (2)*, vol. 62, no. 3, pp. 641–654, 2019, doi: 10.1017/s0013091518000500.

[18] "GAP – Groups, Algorithms, and Programming, Version 4.10.2," 2019. [Online]. Available: https://www.gap-system.org

[19] 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.*, vol. 34, pp. 253–288; ibid. 34 (1970), 475–500, 1970.

[20] J.-P. Serre, "Bases normales autoduales et groupes unitaires en caractéristique 2," *Transform. Groups*, vol. 19, no. 2, pp. 643–698, 2014, doi: 10.1007/s00031-014-9269-6.

[21] Y. Wang and H. Liu, "The unitary subgroups of group algebras of a class of finite p-groups," *Journal of Algebra and Its Applications*, 2021, doi: 10.1142/S0219498823500433.

[22] Y. Wang and H. Liu, "The unitary subgroups of group algebras of a class of finite 2-groups with derived subgroup of order 2," *Science China Mathematics*, pp. 1–29, 2023, doi: 10.1007/s11425-023-2156-7.

Author's address

Zsolt Balogh

Department of Math. Sci, College of Science, United Arab Emirates University, Al Ain, United Arab Emirates,

E-mail address: baloghzsa@gmail.com