http://ijgt.ui.ac.ir/

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 13 No. 2 (2024), pp. 189-194.

www.ui.ac.ir

THE PROBABILITY OF ZERO MULTIPLICATION IN FINITE GROUP ALGEBRAS

HAVAL M. MOHAMMED SALIH

Abstract. Let $\mathbb{F}_qG$ be a finite group algebra. We denote by $P(\mathbb{F}_qG)$ the probability that the product of two elements of $\mathbb{F}_qG$ be zero. In this paper, we obtain several results on this probability including a computing formula and characterizations. In particular, the computing formula for the $P(\mathbb{F}_qG)$ are established where G is the cyclic group C_n, the Quaternion group Q_8, the symmetric group S_3 and F_q is a finite field.

1. Introduction

Throughout this paper, $\mathbb{F}_q$ denotes a finite field with q elements where q is a prime power of p. Let G be a finite non trivial group. Then $\mathbb{F}_qG$ is the group algebra of G over the field $\mathbb{F}_q$. The set of all invertible elements of $\mathbb{F}_qG$ form a group called the unit group of $\mathbb{F}_qG$ denoted by $\mathcal{U}(\mathbb{F}_qG)$. There are many known results about the group unit of $\mathbb{F}_qG$ in [2, 3, 4]. The main topic of this study is to find the nullity degree (probability) of $\mathbb{F}_qG$, which is the probability that the multiplication of two randomly chosen elements of $\mathbb{F}_qG$ is zero. That is

$$P(\mathbb{F}_qG) = \frac{|\{(a,b) \in \mathbb{F}_qG \times \mathbb{F}_qG \ : ab = 0\}|}{|\mathbb{F}_qG|^2}.$$

where $a := \sum_{g\in G} r_g g$ and $b := \sum_{g\in G} \bar{r}_g g$ $(\bar{r}_g, r_g \in \mathbb{F}_q, g \in G)$. Since $\mathbb{F}_qG$ is a finite group ring with identity, then we have that $\mathbb{F}_qG = \{0\} \cup \mathcal{U}(\mathbb{F}_qG) \cup ZD(\mathbb{F}_qG)$, where $ZD(\mathbb{F}_qG)$ is the set of nonzero zero divisors of $\mathbb{F}_qG$. For $x \in \mathbb{F}_qG$, the left (right) annihilator of x is the set $Ann_l(x) = \{\alpha \in \mathbb{F}_qG \ : \alpha x = 0\}$

MSC(2010): Primary: 16S34; Secondary: 16U60.

Keywords: unit, zero divisor, Wedderburn decomposition.

Communicated by Victor Bovdi.

Article Type: Research Paper.

Received: 09 May 2023, Accepted: 07 September 2023.

Cite this article: H. M. Mohammed Salih, The probability of zero multiplication in finite group algebras, Int. J. Group Theory, **13** no. 2 (2024) 189–194. http://dx.doi.org/10.22108/ijgt.2023.137640.1842 .

$(Ann_r(x) = \{\alpha \in \mathbb{F}_qG \ : x\alpha = 0\})$. Similarly we define the annihilator of x by $Ann(x) = \{\alpha \in \mathbb{F}_qG \ : \alpha x = x\alpha = 0\}$. If G is an abelian group, then we can write $P(\mathbb{F}_qG)$ in term of the unit group and zero divisor set as follows:

$$P(\mathbb{F}_qG) = \frac{\sum_{x\in\mathbb{F}_qG} |Ann(x)|}{|\mathbb{F}_qG|^2} \tag{1.1}$$

$$= \frac{|\mathbb{F}_qG| + |\mathcal{U}(\mathbb{F}_qG)| + \sum_{0\neq x\in ZD(\mathbb{F}_qG)} |Ann(x)|}{|\mathbb{F}_qG|^2}, \tag{1.2}$$

If G is non abelian group, then

$$P_l(\mathbb{F}_qG) = \frac{|\mathbb{F}_qG| + |\mathcal{U}(\mathbb{F}_qG)| + \sum_{0\neq x\in ZD(\mathbb{F}_qG)} |Ann_l(x)|}{|\mathbb{F}_qG|^2}$$

The probability of a finite commutative ring R with identity can be found in [1]. Recently in [5], Mohammed Salih derive the general formula for computing $P(\mathbb{F}_qG)$ where $|G| < 5$.

In this paper, $M_n(\mathbb{F}_q)$ denotes the ring of all $n \times n$ matrix over $\mathbb{F}_q$, R denotes a ring with identity. Also $C_n = \langle a|a^n = 1\rangle$ denotes the cyclic group of order n and $R_1 \bigoplus R_2$ denotes direct sum of rings R_1 and R_2. The group that we define below via its presentation is called the Quaternion group of order 8.

$$Q_8 = \langle a, b|a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1}\rangle.$$

2. Background

The following two results are well known [2]. These give us the structure of the unit group of some group algebras $\mathbb{F}_qC_n$.

Theorem 2.1. [2] *If $gcd(n, p) = 1$ and $q = p^m$, then $\mathcal{U}(\mathbb{F}_qC_n) \cong C_{q-1} \times (\prod_{l|n,l>1} C_{q^{d_l}-1}^{el})$ where d_l is the multiplicative order of q modulo l and $e_l = \frac{\varphi(l)}{d_l}$.*

Now consider the case $p|n$.

Lemma 2.2. [2] *Let $k \in \mathbb{N}$. Then* $\mathcal{U}(\mathbb{F}_{p^m}C_{p^k}) \cong \begin{cases} C_{p^m-1} \times C_p^{m(p-1)} & if k = 1 \\ C_{p^m-1} \times \prod_{t=1}^{k} C_{p^t}^{n_t} & otherwise \end{cases}$

where $n_k = m(p-1)$ and $n_t = mp^{k-t-1}(p-1)^2$, for all $t, 1 \leq t < k$.

The next three results tell us the group algebra KG has Wedderburn decomposition of the form.

Proposition 2.3. [6] *Let G be an abelian group of order n and K a field such that the characteristic of the field does not divide n. If K contains a primitive root of unity of order n, then $KG \cong K \bigoplus \cdots \bigoplus_{n\text{-}times} K$.*

Proposition 2.4. [6] *Let F be a finite field where the characteristic of the field is not equal to 2. Then $FQ_8 = F \bigoplus F \bigoplus F \bigoplus F \bigoplus M_2(F)$ if and only if $x^2 + y^2 = -1$ can be solved in F.*

http://dx.doi.org/10.22108/ijgt.2023.137640.1842

Proposition 2.5. [8] *Let $\mathbb{F}_q$ be a finite field and $gcd(q,6)=1$. Then $\mathbb{F}_qS_3 \cong \mathbb{F}_q \bigoplus \mathbb{F}_q \bigoplus M_2(\mathbb{F}_q)$.*

Theorem 2.6. [5] *Let RG be a finite group ring. Then $P(RG) \geq \frac{1}{4}$ if and only if RG is isomorphic to one of the following rings: $\mathbb{Z}_2C_2, \mathbb{Z}_3C_2, \mathbb{Z}_2C_3$.*

Initially, it was challenging for us to derive a computing formula for $P(\mathbb{F}_qG)$, since there is no analogous concept of it. Finally, we are able to get the formula for $P(\mathbb{F}_qG)$, where $|G| < 5$ in [5]. In this paper, it may be pointed out that for most of these group algebras, the GAP program fails to compute the $P(\mathbb{F}_qG)$ if $|G| \geq 6$, then the program may crash, even by using super computer. So we need to solve this problem by using algebraic tools. Further, we provide the explicit formula of $P(\mathbb{F}_qC_n)$, if $gcd(n,p)=1$. Also we find the $P(\mathbb{F}_qG)$ where $G = S_3$ or Q_8 for some cases by using the Wedderburn decomposition.

3. The general formula of the probability of some group algebras $\mathbb{F}_qG$

In this section, we get serveral results for $P(\mathbb{F}_qG)$ and derive a computing formula for $P(\mathbb{F}_qG)$. We begin with the following result:

Lemma 3.1. *Let $R_1, \ldots, R_n$ be finite rings. Then $P(R_1 \bigoplus R_2 \bigoplus \cdots \bigoplus R_n) = P(R_1)P(R_2)\cdots P(R_n)$.*

Proof. It is straightforward. □

Theorem 3.2. *If $gcd(n,p)=1$ and $q=p^m$, then $P(\mathbb{F}_qC_n) = (\frac{2q-1}{q^2}) \times \prod_{l|n\ l>1}(\frac{2q^{d_l}-1}{q^{2d_l}})^{e_l}$ where d_l is the multiplicative order of q module l and $e_l = \frac{\phi(l)}{d_l}$, ϕ denotes the Euler Totient function.*

Proof. Using [10, Theorem 1] and [9, Theorem 2.21, pp.53], it follows that $\mathbb{F}_qC_n \cong \mathbb{F}_q \bigoplus (\bigoplus_{l|n\ l>1} \mathbb{F}_{q^{d_l}}^{e_l})$. By Lemma 3.1 and [1, Lemma 3.1], the result follows. □

Note that, we are going to use Perlis-Walker Theorem in order to determine how many elements has annihilator of size q^l.

Theorem 3.3. *Let $\mathbb{F}_q$ be a field of characteristic p, where $q=p^m$. Then*

$$P(\mathbb{F}_qC_5) \cong \begin{cases} \frac{q^7-q^6+q^5+q^4-q^2+q-1}{q^9} & if\ p|5. \\ \frac{4q^5-2q^4-2q+1}{q^{10}} & q \equiv 2 \text{ or } 3 \mod 5 \text{ and if } gcd(p,5)=1. \\ \frac{q^6-2q^3+5q^2-2q-1}{q^8} & q \equiv 4 \mod 5 \text{ and if } gcd(p,5)=1. \\ \frac{2q^6+5q^5-21q^4+35q^3-29q^2+10q-1}{q^{10}} & q \equiv 1 \mod 5 \text{ and if } gcd(p,5)=1. \end{cases}$$

Proof. Let $v \in ZD(\mathbb{F}_qC_5) \setminus \{0\}$ and $\psi\colon \mathbb{F}_qC_5 \to \mathbb{F}_qC_5$ the $\mathbb{F}_q$-linear transformation defined $\psi(x) = vx$, then $Ann(x) = Ker\psi$ that a non trivial $\mathbb{F}_q$-linear subspace of dimension $1 \leq l \leq 4$. That is $|Ann(x)| = q, q^2, q^3$ or q^4. We have four cases to analysis:

Case 1, If $q \cong 0 \mod 5$, then there are $q-1, q(q-1), q^2(q-1), q^3(q-1)$ elements $0 \neq x \in ZD(\mathbb{F}_qC_5)$ such that $|Ann(x)| = q, q^2, q^3, q^4$. By Lemma 2.2, we obtain $|\mathcal{U}(\mathbb{F}_qC_5)| = q^4(q-1)$.

http://dx.doi.org/10.22108/ijgt.2023.137640.1842

Case 2, if $q \cong 2 \mod 5$ or $q \cong 3 \mod 5$, there are $q^4-1, 0, 0, (q-1)$ elements $0 \neq x \in ZD(\mathbb{F}_qC_5)$ such that $|Ann(x)| = q, q^2, q^3, q^4$. Also, by Theorem 2.1, we obtain $|\mathcal{U}(\mathbb{F}_qC_5)| = (q^4-1)(q-1)$.

Case 3, if $q \cong 4 \mod 5$, then there are $q-1, 2(q^2-1), 2(q^2-1)(q-1), (q^2-1)^2$ elements $0 \neq x \in ZD(\mathbb{F}_qC_5)$ such that $|Ann(x)| = q, q^2, q^3, q^4$. So $|\mathcal{U}(\mathbb{F}_qC_5)| = (q^2-1)^2q$ by Theorem 2.1.

Case 4, if $q \cong 1 \mod 5$, then there are $5(q-1)^4, (q-1)^4, (q-1)^3, 5(q-1)$ elements $0 \neq x \in ZD(\mathbb{F}_qC_5)$ such that $|Ann(x)| = q, q^2, q^3, q^4$. So $|\mathcal{U}(\mathbb{F}_qC_5)| = (q-1)^5$ by Theorem 2.1.

The rest follows from Equation (1.2). □

Remark 3.4. *We can see that the proof of the cases 2,3 and 4 in Theorem 3.3 follows from Theorem 3.2.*

Theorem 3.5. *Let RG be a finite group algebra with identity such that $P(RG) \geq \frac{1}{10}$. Then the structure of RG and the possible values of $P(RG)$ are given in Table 1.*

TABLE 1. All group algebras with $P(RG) \geq 0.1$

n	RG	$P(RG)$
1	$\mathbb{F}_2C_2$	$\frac{1}{2} = 0.5$
2	$\mathbb{F}_3C_2$	$\frac{25}{81} \simeq 0.308$
3	$\mathbb{F}_5C_2$	$\frac{81}{625} \simeq 0.129$
4	$\mathbb{F}_2C_3$	$\frac{21}{64} \simeq 0.328$
5	$\mathbb{F}_2C_4$	$\frac{3}{36} \simeq 0.18$
6	$\mathbb{F}_3C_3$	$\frac{1}{9} \simeq 0.111$
7	$\mathbb{F}_4C_2$	$\frac{5}{32} \simeq 0.156$
8	$\mathbb{F}_2(C_2 \times C_2)$	$\frac{7}{32} \simeq 0.218$
9	$\mathbb{Z}_4C_2$	$\frac{7}{32} \simeq 0.218$
10	$\mathbb{Z}_6C_2$	$\frac{25}{162} \simeq 0.154$
11	$\mathbb{F}_2S_3$	$\frac{5}{64} \simeq 0.113$

Proof. The proof follows from direct computations and [5, Theorems 3.1, 3.2, 3.3 and 3.4]. □

A direct consequence of Theorem 3.5 is the following result.

Corollary 3.6. *Let RG be a finite group algebras with identity. Then the following holds:*

(1) $P(RG) \notin (\frac{21}{64}, \frac{1}{4})$.
(2) *If $RG \ncong \mathbb{F}_2C_2, \mathbb{F}_2C_3$, then $P(RG) \leq \frac{21}{64}$. Moreover, the equality holds if and only if $RG \cong \mathbb{F}_2C_3$.*
(3) *If $RG \ncong \mathbb{F}_3C_2, \mathbb{F}_2C_2, \mathbb{F}_2C_3$, then $P(RG) < \frac{2}{10}$.*
(4) $P(RG) = \frac{7}{32}$ *if and only if $RG \cong \mathbb{F}_2(C_2 \times C_2), \mathbb{F}_5C_2$.*

Proposition 3.7. *If $R = M_2(\mathbb{F}_q)$ the algebra 2 by 2 matrices over $\mathbb{F}_q$, then $P_l(R) = \frac{q^4+3q^3-2q(q+1)+1}{q^7}$.*

http://dx.doi.org/10.22108/ijgt.2023.137640.1842

Proof. By the same idea as in proof of Theorem 3.3, we have $|Ann_l(x)| = q^2$ for all $0 \neq x \in ZD(R)$. By using [7, Theorem 3.1], we obtain $\mathcal{U} = q(q^3 - q^2 - q + 1)$. Since R is finite ring with identity, then $R = \{0\} \cup \mathcal{U} \cup ZD(R)$. So there are $q^3 + q^2 - q - 1$ elements $0 \neq x \in ZD(R)$ of size $|Ann(x)| = q^2$. So $\sum_{0 \neq x \in ZD(R)} |Ann_l(x)| = q^2(q^3 + q^2 - q - 1)$. Put these equations in Equation (1.2) and the result follows. □

Proposition 3.8. *If $R = M_2(\mathbb{F}_q)$ the algebra 2 by 2 matrices over $\mathbb{F}_q$, then $P(R) = \frac{3q^2-2}{q^6}$.*

Proof. By the same idea as in proof of Theorem 3.3, we have $|Ann_l(x)| = q$ for all $0 \neq x \in ZD(R)$. The rest is similar as the proof of Proposition 3.7. □

Theorem 3.9. *Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2$. Then*

(1) $P_l(\mathbb{F}_qQ_8) = (\frac{2q-1}{q^2})^4 \times (\frac{q^4+3q^3-2q^2-2q+1}{q^7})$.
(2) $P(\mathbb{F}_qQ_8) = (\frac{2q-1}{q^2})^4 \times (\frac{3q^2-2}{q^6})$.

Proof. Since $\mathbb{F}_q$ is a finite field of characteristic $p \neq 2$. Then by Proposition 2.4, we have $\mathbb{F}_qQ_8 = \mathbb{F}_q \bigoplus \mathbb{F}_q \bigoplus \mathbb{F}_q \bigoplus \mathbb{F}_q \bigoplus M_2(\mathbb{F}_q)$.

(1) From Lemma 3.1, [1, Lemma 3.1] and Proposition 3.7, the result follows.
(2) From Lemma 3.1, [1, Lemma 3.1] and Proposition 3.8, the result follows.

□

Theorem 3.10. *Let $\mathbb{F}_q$ be a finite field and $gcd(q, 6) = 1$. Then*

(1) $P_l(\mathbb{F}_qS_3) = (\frac{2q-1}{q^2})^2 \times (\frac{q^4+3q^3-2q^2-2q+1}{q^7})$.
(2) $P(\mathbb{F}_qS_3) = (\frac{2q-1}{q^2})^2 \times (\frac{3q^2-2}{q^6})$.

Proof. The proof is similar as Theorem 3.9. □

Proposition 3.11. *Let $\mathbb{F}_q$ be a finite field of characteristic 2. Then*

(1) $P_l(\mathbb{F}_qS_3) = \frac{3q^5+7q^4-12q^3-2q^2+7q-2}{q^{10}}$.
(2) $P(\mathbb{F}_qS_3) = \frac{9q^3-6q^2-6q+4}{q^9}$.
(3) $P(\mathbb{F}_qQ_8) = \frac{3q^2+3q-5}{q^9}$.

Proof. Clear. □

Example 3.12. *Consider the finite field $\mathbb{F}_7$, the symmetric group S_3 and the cyclic group C_6. The probability $P_l(\mathbb{F}_7S_3)$ and $P(\mathbb{F}_7C_6)$ cannot compute by personal computer. So we use super computer with property* ***Intel®Xeon®Platinum 8280 CPU@ 2.70GHz 2.69GHz Installed RAM 128GB (128GB usable)****. The computation takes nearly 129 hours and the outputs are the following:*

On the other hand, we achieve this computation with a few seconds by using Theorem 3.10, part 1 and Theorem 3.2.

http://dx.doi.org/10.22108/ijgt.2023.137640.1842

TABLE 2. $|Ann_l(x)|$ and number of elements of size $|Ann_l(x)|$

$\|Ann_l(x)\|$	*1*	*7*	*49*	*343*	*2401*	*16807*	*117649*
F_7S_3	*72576*	*24192*	*15840*	*4608*	*420*	*12*	*1*
F_7C_6	*46656*	*46656*	*19440*	*4320*	*540*	*36*	*1*

Acknowledgments

I would like thank to the referee for careful reading of the article and detailed report including corrections and comments; and I appreciate his/her effort on reviewing the article.

REFERENCES

[1] M. A. Esmkhani and S. M. Jafarian Amiri, The probability that the multiplication of two ring elements is zero, *J. Algebra Appl.*, **17** (2018) 9 pp.

[2] N. Makhijani, R. K. Sharma and J. B. Srivastava, The unit group of algebra of circulant matrices, *Int. J. Group Theory*, **3** no. 4 (2014) 13–16.

[3] J. Gildea, On the order of $U(F_{p^k}D_{2p^m})$, *Int. J. Pure Appl. Math.*, **46** (2008) 267–272.

[4] G. Tang and Y. Gao, The unit groups of FG of groups with order 12, *Int. J. Pure Appl. Math.*, **73** (2011) 143–158.

[5] H. M. Mohammed Salih, On the probability of zero divisor elements in group rings *Int. J. Group Theory*, **11** no. 4 (2022) 253–257.

[6] C. P. Milies and S. K. Sehgal, *An introduction to group rings*, Springer Science and Business Media, **1**, Kluwer Academic publishers Dordrecht/Boston/London, 2002.

[7] H. Cheraghpour and N. G. Ghosseiri, On the idempotents, nilpotents, units and zero-divisors of finite rings. *Linear Multilinear Algebra*, **67** (2019) 327–336.

[8] F. E. Brochero Martinez, Structure of finite dihedral group algebra, *Finite Fields Appl.*, **35** (2015) 204-214.

[9] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, 1997.

[10] S. Perlis and G. L. Walker, Abelian group algebras of finite order, *Trans. Amer. Math. Soc.*, **68** (1950) 420–426.

[11] D. David, The probability of zero multiplication in finite rings, *Bull. Aust. Math. Soc.*, **106** (2022) 83–88.

Haval M. Mohammed Salih

Department of Mathematics, Faculty of Science, Soran University , Kawa St, Soran, Erbil, Iraq

Email: havalmahmood07gmail.com