

有限环的乘法概率

DAVID DOLŽAN

ABSTRACT. 我们研究在一个有限环 R 中随机选取两个元素的乘积等于某个固定元素 $x \in R$ 的概率。我们计算了半单环和某些特殊局部环类别的这一概率，并找到了任意有限环中该概率的界限。

1. 介绍

离散概率相关的问题历史上首先是在群的背景下进行研究的，参见例如 [2, 11, 12, 14, 19]。后来，研究人员在环的研究中也进行了类似的研究。作者们研究了交换概率（也称为交换度）（参见 [3, 4, 5, 7, 8, 15, 20]）和零乘法概率（也称为零度）（参见 [6, 9, 10, 16, 20]）的有限环。最近，[18] 和 [21] 中的作者解决了寻找由 $\text{Prob}_x(R) = \frac{|\{(a,b) \in R^2; ab=x\}|}{|R|^2}$ 定义的有限环的乘法概率的问题，其中 $x \in R$ 是任意元素。显然，这是零度的一种推广，因此这种概率有时也被称为有限环的广义概率。然而，在 [18, 21] 中的作者仅在交换环的背景下解决了这个问题，他们主要关注模 n 的一些固定整数 n 的环。

在本文中，我们研究了任意有限环的广义概率。在下一节中，我们将收集一些定义和初步结果，这些将在论文中派上用场。我们还建立了乘法概率的界限（参见引理 2.4），从而推广了 [6, Theorem 4.1] 和 [18, Theorem 2.1] 中的陈述。我们还计算了环直积的乘法概率，并找到了一个环及其雅可比根上的商环的乘法概率之间的关系。在第 3 节中，我们找到了简单环的乘法概率（参见定理 3.2）。在最后一节中，我们研究了局部环的乘法概率。首先，我们建立了界限并检查这些界限何时达到（参见定理 4.2 和推论 4.3）。然后我们计算两类特殊的有限局部环中的乘法概率：这类环的雅各布森根 J 具有可能的最大幂零指数（参见定理 4.6）——这样的环类包含例如所有形如 $\mathbb{Z}_n$ 的环，其中 n 是一个素数的幂次，因此定理 4.6 是 [21, Theorem 2.1 and Theorem 2.2] 的一个推广，也包括那些满足 $J^2 = 0$ 条件的环（参见定理 4.7）。

2020 *Mathematics Subject Classification.* 16P10, 16L30, 16K20.

Key words and phrases. 有限环；雅各布森根；概率。

The author acknowledges the financial support from the Slovenian Research Agency (research core funding No. P1-0222).

2. 定义和预备知识

在整个论文中, R 表示一个具有单位元的有限环 1。我们将它的单位群表示为 R^* , 零因子集表示为 $Z(R) = \{x \in R; \text{there exists } 0 \neq y \in R \text{ such that } xy = 0 \text{ or } yx = 0\}$, 雅各布森根表示为 $J(R)$ 。当所讨论的环无疑时, 我们将简单地写作 J 而不是 $J(R)$ 。我们将经常用 $\bar{x} = x + J$ 表示 x 在 R/J 中的等价类。元素 $x \in R$ 的 (右) 零化子将表示为 $\text{Ann}_r(x) = \{y \in R; xy = 0\}$ 。如果所讨论的环不明显, 我们将写 $\text{Ann}_r(x, R)$ 而不是 $\text{Ann}_r(x)$ 。

我们将记 $M_n(F)$ 为域 F 上的 n -by- n 矩阵的环, 并将 $A \in M_n(F)$ 的秩记为 $\text{rk}(A)$ 。

我们将利用以下简单引理, 该引理表明在有限环中, 每个左零因子也是右零因子 (反之亦然)。

引理 2.1. [13, Proposition 1.3] 令 R 为一个有限环, 并且 $a \in R$ 。如果存在 $0 \neq b \in R$ 使得 $ba = 0$, 那么存在 $0 \neq c \in R$ 使得 $ac = 0$ 。

为了计算广义概率, 我们有以下定义。

定义 2.2. 令 $a, x \in R$ 。我们定义

$$\delta_x(a) = \begin{cases} 1, & \text{if there exists } b \in R \text{ such that } ab = x, \\ 0, & \text{otherwise.} \end{cases}$$

我们立即得到以下引理。

引理 2.3. 设 R 是一个有限环。对于 $x \in R$, 我们有 $\text{Prob}_x(R) = \frac{\sum_{a \in R} |\text{Ann}_r(a)| \delta_x(a)}{|R|^2}$ 。

Proof. 假设存在 $b \in R$, 使得 $ab = x$ 。现在, $ac = x$ 意味着 $a(c - b) = 0$, 所以 $c - b \in \text{Ann}_r(a)$ 。因此, 对于所有确切的 $c \in b + \text{Ann}_r(a)$, $ac = x$ 成立。 ■

以下引理是 [6, Theorem 4.1] 和 [18, Theorem 2.1] 的推广。请注意, $\text{Prob}_0(R) \leq \frac{2|R| - 2|Z(R)| + |Z(R)|^2}{|R|^2}$ 已经在 [6, Theorem 4.1] 中被证明。

引理 2.4. 如果 R 是一个有限环, 则 $x \in R^*$ 当且仅当 $\text{Prob}_x(R) = \frac{|R^*|}{|R|^2}$ 。此外, 如果 $0 \neq x \notin R^*$, 则 $\frac{|R^*|}{|R|^2} \cdot \frac{2 + |Z(R)|}{|Z(R)|} \leq \text{Prob}_x(R) \leq \frac{|R| - 2|Z(R)| + |Z(R)|^2}{|R|^2}$ 和 $\frac{2|R| + |Z(R)| - 2}{|R|^2} \leq \text{Prob}_0(R) \leq \frac{2|R| - 2|Z(R)| + |Z(R)|^2}{|R|^2}$ 。

Proof. 表示 $A = \{(a, b) \in R^2; ab = x\}$ 。首先假设 $x \in R^*$ 。由于, $ab = x$ 当且仅当 $x^{-1}ab = 1$, 我们看到 $(a, b) \in A$ 当且仅当 $b \in R^*$ 和 $(xb^{-1}, b) \in A$, 所以 $|A| = |R^*|$ 并因此 $\text{Prob}_x(R) = \frac{|A|}{|R|^2} = \frac{|R^*|}{|R|^2}$ 。如果 $x = 0$, 则对于每一个 $b \in R$ 和每一个 $a \in R$ 都有 $(0, b), (a, 0) \in A$ 。然而, 如果 $0 \neq a \in Z(R)$, 则由引理 2.1 可知 $|\text{Ann}_r(a)| \geq 2$, 所以

$|A| \geq |R| + |R^*| + 2(|Z(R)| - 1) = 2|R| + |Z(R)| - 2$, 下界由此得出。上界由 [6, Theorem 4.1] 得出。注意在这种情况下, $|A| > |R^*|$, 因此 $\text{Prob}_x(R) \neq \frac{|R^*|}{|R|^2}$ 。最后, 假设 $0 \neq x \in Z(R)$ 。如果 $a \in R^*$, 则对于每一个 $t \in \text{Ann}_r(xa)$ 都有 $(a, a^{-1}x), (xa, a^{-1} + t) \in A$ 。由于 $xa \in Z(R)$, 根据引理 2.1 我们得到 $|\text{Ann}_r(xa)| \geq 2$ 。如果对于某些 $a, b \in R^*$ 有 $xa = xb$, 则 $x(a-b) = 0$, 所以 $a-b \in Z(R)$ 。因此存在 $z \in Z(R)$ 使得 $a = b + z$ 。这表明我们至少有 $\frac{|R^*|}{|Z(R)|}$ 个不同的元素 xa , 因此 $|A| \geq |R^*| + \frac{2|R^*|}{|Z(R)|}$ 并且从而 $\text{Prob}_x(R) \geq \frac{|R^*|}{|R|^2} \cdot \frac{2+|Z(R)|}{|Z(R)|}$ 。注意在这种情况下, $|A| > |R^*|$ 因此 $\text{Prob}_x(R) \neq \frac{|R^*|}{|R|^2}$ 。由于 R 的每个元素要么是单位元要么是零因子, 这现在证明了 $x \in R^*$ 当且仅当 $\text{Prob}_x(R) = \frac{|R^*|}{|R|^2}$ 。为了证明上限, 观察到对于 $a \in R^*$, 我们有 $|\text{Ann}_r(a)| = 1$ 和 $\delta_x(a) = 1$, $\delta_x(0) = 0$, 而对于 $0 \neq a \in Z(R)$, 我们有 $\delta_x(a) \leq 1$ 和 $|\text{Ann}_r(a)| \leq |Z(R)|$, 因此 $|A| \leq |R^*| + |Z(R)|(|Z(R)| - 1)$ 。 ■

以下引理表明我们可以始终将研究范围限制在直接不可分解环的乘法概率上。

引理 2.5. 如果 $R = R_1 \times R_2 \times \dots \times R_n$ 是有限环和 $x = (x_1, x_2, \dots, x_n) \in R$ 的直积, 则 $\text{Prob}_x(R) = \prod_{i=1}^n \text{Prob}_{x_i}(R_i)$ 。

Proof. 注意到对于任何元素 $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n)$ 和 $x = (x_1, x_2, \dots, x_n) \in R$, 我们有 $ab = x$ 当且仅当对于每一个 $i = 1, 2, \dots, n$ 都有 $a_i b_i = x_i$ 。 ■

我们以以下估计结束这一初步部分。

引理 2.6. 令 R 是一个有限环, I 是 R 的一个真理想。对于任意的 $x \in R$, 我们有 $\text{Prob}_x(R) \leq \text{Prob}_{x+I}(R/I)$ 。

Proof. 我们由引理 2.3 得到 $\text{Prob}_x(R) = \frac{\sum_{a \in R} |\text{Ann}_r(a)| \delta_x(a)}{|R|^2}$ 。由于 $\delta_x(a) = 1$ 蕴含 $\delta_{x+I}(a+I) = 1$, 并且对于 $\text{Ann}_r(a, R)$ 中的任何 $|I|$ 元素, 我们在 $\text{Ann}_r(a+I, R/I)$ 中至少有一个元素, 我们得到 $\text{Prob}_x(R) \leq \frac{\sum_{a \in R} |\text{Ann}_r(a+I, R/I)| |I| \delta_{x+I}(a+I)}{|R|^2} = \frac{\sum_{a+I \in R/I} |\text{Ann}_r(a+I, R/I)| |I|^2 \delta_{x+I}(a+I)}{|R|^2} = \text{Prob}_{x+I}(R/I)$ 。 ■

3. 单环

在本节中, 我们研究任意 (半) 单有限环的乘法概率。引理 2.5 表明, 为了计算半单环的乘法概率, 我们必须研究单环的乘法概率, 因此我们将自己限制在这种特殊情况。

由于包含某个子空间 U 的 F^n 中的 k 维子空间与商空间 $F^n/U \simeq F^{n-r}$ 中的 $(k-r)$ 维子空间具有一一对应关系, 我们立即得到以下引理。

引理 3.1. [1, Theorem 13.1] 令 F 是一个含有 q 元素的有限域, 并且令 $r \leq k \leq n$ 是整数。如果 U 是 F^n 中的一个 r 维子空间, 那么在 F^n 中恰好存在 $\prod_{i=0}^{k-r-1} \frac{q^{n-r}-q^i}{q^{k-r}-q^i}$ k 维的子空间包含 U 。

我们现在有如下定理。

定理 3.2. 令 F 为一个包含 q 个元素的有限域, n 是一个整数。对于秩为 $r \leq n$ 的矩阵 $X \in M_n(F)$, 我们有

$$\text{Prob}_X(M_n(F)) = \sum_{k=r}^n \frac{\prod_{i=0}^{k-r-1} \frac{q^{n-r}-q^i}{q^{k-r}-q^i} \prod_{i=0}^{k-1} (q^n - q^i)}{q^{n(n+k)}}.$$

Proof. 由引理 2.3, 我们有 $\text{Prob}_X(R) = \frac{\sum_{k=0}^n \sum_{\text{rk}(A)=k} |\text{Ann}_r(A)| \delta_X(A)}{|R|^2}$ 。注意存在 $B \in M_n(F)$ 使得 $AB = X$ 当且仅当 X 的列空间是 A 列空间的子空间。记 X 的列空间为 U 。由于 $\text{rk}(X) = r$, 我们需要计算所有秩为 $k \geq r$ 的矩阵 A , 使得它们的列空间包含 U 。由引理 3.1 可知, 在 F^n 中存在恰好包含 U 的 $\prod_{i=0}^{k-r-1} \frac{q^{n-r}-q^i}{q^{k-r}-q^i}$ k 维子空间。选择任意这样的子空间 V 。现在, 我们有与列空间等于 V 的矩阵数量一样多的满射映射从 F^n 到 V , 这正是 $(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})$ 。因此, 恰好有 $\prod_{i=0}^{k-r-1} \frac{q^{n-r}-q^i}{q^{k-r}-q^i} \prod_{i=0}^{k-1} (q^n - q^i)$ 个秩为 k 的矩阵 A , 使得 $\delta_X(A) = 1$ 。选择 $x \in F^n$ 。由于任何秩为 k 的矩阵 A , 使得方程 $Ay = x$ 可解, 恰好有 q^{n-k} 个解 $y \in F^n$, 我们看到存在确切地 $(q^{n-k})^n$ 个矩阵 B , 使得对于任何满足 $\delta_X(A) = 1$ 的 $A \in M_n(F)$ 都有 $AB = X$ 。这表明

$$\text{Prob}_X(M_n(F)) = \frac{\sum_{k=r}^n q^{n(n-k)} \prod_{i=0}^{k-r-1} \frac{q^{n-r}-q^i}{q^{k-r}-q^i} \prod_{i=0}^{k-1} (q^n - q^i)}{q^{2n^2}},$$

, 从而证明了该定理。 ■

4. 局部环

在本节中, 我们将研究局部有限环的乘法概率。我们需要以下引理。

引理 4.1. [17, Theorem 2] 令 R 是一个有限局部环, 具有 $|R| = q^n$ 和 $R/J = GF(q)$ 。令 I 是 R 中的一个左 (右) 理想。则存在整数 α , 使得 $|I| = q^\alpha$ 。此外, 存在 $g \in R^*$ 使得 $g + J$ 是域 R/J 的本原元素, 并且对于某个 $k, l \in \{0, 1, \dots, q-1\}$ 有 $g^k - g^l \in J$ 蕴含 $k = l$ 。

从引理 2.4, 我们现在得到以下结果。

定理 4.2. 令 R 为一个有限局部环, 其中 $|R| = q^n$ 对于某些 $n \geq 2$ 和 $R/J = GF(q)$ 成立。那么 $x \in R^*$ 当且仅当 $\text{Prob}_x(R) = \frac{q-1}{q^{n+1}}$ 。此外, 如果 $0 \neq x \in J$, 则 $\frac{(q-1)(q^{n-2}+1)}{q^{2n-1}} \leq \text{Prob}_x(R) \leq \frac{q^{n-1}+q-2}{q^{n+1}}$ 和 $\frac{3q^{n-1}-q^{n-2}-1}{q^{2n-1}} \leq \text{Prob}_0(R) \leq \frac{q^{n-1}+2q-2}{q^{n+1}}$ 。

Proof. 对于 $x \in R^*$, 该陈述直接来自引理 2.4。如果 $x = 0$, 则对于每一个 $b \in R$ 和每一个 $a \in R^*$ 都有 $(0, b), (a, 0) \in A$ 。然而, 如果 $0 \neq a \in J$, 则由引理 2.1 可知 $\text{Ann}_r(a) \neq \{0\}$, 所以由引理 4.1 可知 $|\text{Ann}_r(a)| \geq q$ 。因此 $|A| \geq |R| + |R^*| + q(|J| - 1) = 2|R| + (q - 1)|J| - q$, 所以 $\text{Prob}_0(R) \geq \frac{3q^{n-1} - q^{n-2} - 1}{q^{2n-1}}$ 。上界由引理 2.4 和事实 $|Z(R)| = |J| = q^{n-1}$ 得出。最后, 假设 $0 \neq x \in J$ 。如果 $a \in R^*$, 那么对于每一个 $t \in \text{Ann}_r(xa)$ 都有 $(a, a^{-1}x), (xa, a^{-1} + t) \in A$ 。由于 $\text{Ann}_r(xa)$ 是非平凡的, 我们有 $|\text{Ann}_r(xa)| \geq q$ 根据引理 4.1。现在, 如果 $xa = xb$ 对某些 $a, b \in R^*$ 成立, 则 $x(a - b) = 0$, 因此 $a - b \in J$ 。因此至少存在 $q - 1$ 个不同的元素 xa , 所以 $|A| \geq |R^*| + q(q - 1)$, 从而 $\text{Prob}_x(R) \geq \frac{(q-1)(q^{n-1}+q)}{q^{2n}} = \frac{(q-1)(q^{n-2}+1)}{q^{2n-1}}$ 。上界再次直接来自引理 2.4。 ■

接下来的两个推论向我们展示了这些界限何时恰好被达到。

推论 4.3. 令 R 是一个有限局部环, 满足 $|R| = q^n$ 对某个 $n \geq 2$ 和 $R/J = GF(q)$ 成立。下列陈述是等价的。

- (1) $\text{Prob}_x(R) = \frac{(q-1)(q^{n-2}+1)}{q^{2n-1}}$ 对于每一个 $0 \neq x \in J$ 。
- (2) $\text{Prob}_x(R) = \frac{q^{n-1}+q-2}{q^{n+1}}$ 对于每一个 $0 \neq x \in J$ 。
- (3) $\text{Prob}_0(R) = \frac{3q^{n-1}-q^{n-2}-1}{q^{2n-1}}$ 。
- (4) R 是一个包含 q^2 个元素的环。

Proof. (1) $\Rightarrow$ (4): 根据定理 4.2 的证明, 我们看到 $|\text{Ann}_r(x)| = q$ 并且 $x = ab$ 意味着要么是 $a \in R^*$ 要么是 $b \in R^*$ 。由于这对任何 $x \in J$ 都成立, 我们有 $J^2 = 0$ 。 $|\text{Ann}_r(x)| = q$ 现在意味着 $|J| = q$, 因此 $|R| = q^2$ 。

(2) $\Rightarrow$ (4): 引理 2.4 的证明表明, 对于任意的 $0 \neq a \in J$, 我们有 $|\text{Ann}_r(a)| = |J|$, 这意味着 $J^2 = 0$ 。我们还有对于每一个 $0 \neq a \in J$ 都有 $\delta_x(a) = 1$, 这意味着对于每一个 $0 \neq a \in J$ 都存在一个 $u_a \in R^*$ 使得 $au_a = x$, 所以 $a = xu_a^{-1}$ 。但如果 $u_1 - u_2 \in J$, 则 $xu_1 = xu_2$, 所以 $|xR| \leq q$, 这意味着 $|J| = q$, 因此 $|R| = q^2$ 。(3) $\Rightarrow$ (4): 我们知道对于每一个 $0 \neq a \in J$, 由定理 4.2 的证明可得 $|\text{Ann}_r(a)| = q$ 。假设 $J^k \neq 0$ 和 $J^{k+1} = 0$ 对于某个整数 k 。然后由引理 4.1 可知 $|J^k| \geq q$ 。如果 $k \geq 2$, 那么 $|J| > q^2$, 因此存在 $a \in J^k$ 使得 $|\text{Ann}_r(a)| \geq q^2$, 这产生了一个矛盾。我们已经证明了 $J^2 = 0$ 。由于对于每一个 $a \in J$ 和 $aJ = 0$ 都有 $|\text{Ann}_r(a)| = q$, 这表明 $|J| = q$, 因此 $|R| = q^2$ 。

(4) $\Rightarrow$ (1), (2), (3): 如果 $|R| = q^2$, 那么 $|J| = q$ 和 $J^2 = 0$, 因此对于每一个 $0 \neq a \in J$ 都有 $|\text{Ann}_r(a)| = q$ 。现在, 很容易检查定理 4.2 的证明中所有的不等式实际上是等式, 所以 (1) 和 (3) 直接成立。观察还可以发现当 $n = 2$ 时, 陈述 (1) 和 (2) 是相等的, 因此 (2) 也成立。 ■

推论 4.4. 设 R 是一个有限局部环, 具有 $|R| = q^n$ 和 $R/J = GF(q)$ 。则 $\text{Prob}_0(R) = \frac{q^{n-1}+2q-2}{q^{n+1}}$ 当且仅当 $J^2 = 0$ 。

Proof. 这直接来自 [6, Theorem 4.1]。 ■

在局部环的一些特殊情况下，我们实际上可以计算所有的乘法概率。我们需要以下引理。

引理 4.5. 令 R 为有限环，并设 $u \in R^*$ 和 $j \in J$ 。则 $u + j \in R^*$ 。

Proof. 注意 $u + j = u(1 + u^{-1}j)$ 和 $j' = u^{-1}j \in J$ 。由于 J 的每个元素都是幂零的，我们有 $j'^n = 0$ 对于某个整数 n ，因此 $(1 + j')^{-1} = 1 - j' + (j')^2 - \dots + (-1)^{n-1}(j')^{n-1}$ 。■

我们现在有以下定理，该定理推广了来自 [21] 的定理 2.1 和 2.2。

定理 4.6. 令 R 为一个有限局部环，具有 $|R| = q^n$ 和 $R/J = GF(q)$ ，假设 $J^{n-1} \neq 0$ 。如果对于某个整数 k 有 $x \in J^k \setminus J^{k+1}$ ，则 $\text{Prob}_x(R) = \frac{(k+1)(q-1)}{q^{n+1}}$ 。此外， $\text{Prob}_0(R) = \frac{(n+1)q-n}{q^{n+1}}$ 。

Proof. 如果对于某些 i ， $J^i = J^{i+1}$ ，则由 Nakayama 引理可知 $J^i = 0$ 。因此， $J \supset J^2 \supset \dots \supset J^{n-1} \supset 0$ 是一个严格递减的理想链。表示 $J^0 = R$ 并观察对于每一个 $i = 0, 1, \dots, n-1$ ，我们都有 J^i/J^{i+1} 是一个（非平凡的）左 R/J 向量空间，标量乘法定义为 $(x + J)(j + J^{i+1}) = xj + J^{i+1}$ 。这表明对于某个正整数 k_i ，有 $|J^i| = |J^{i+1}|q^{k_i}$ ，因此 $q^n = |R| = q^{k_0+k_2+\dots+k_{n-1}}$ ，当然这就意味着 $k_0 = k_1 = \dots = k_{n-1} = 1$ 。这显示了对于每一个 $i = 0, 1, \dots, n$ 都有 $|J^i| = q^{n-i}$ 。令 $g \in R^*$ 为来自引理 4.1 的元素。现在，对每一个 $i \in \{1, 2, \dots, n-1\}$ 选择 $x_i \in J^i \setminus J^{i+1}$ 。同时也选择任意的 $k \in \{0, 1, \dots, n-1\}$ 并观察 $X_k = \{\sum_{i=k}^{n-1} \lambda_i x_i; \lambda_i \in \{0, g, g^2, \dots, g^{q-1}\} \text{ for every } i \in \{k, k+1, \dots, n-1\}\} \subseteq J^k$ 。我们用归纳法证明当

$$(1) \quad \sum_{i=k}^{n-1} \lambda_i x_i = \sum_{i=k}^{n-1} \mu_i x_i$$

中，对于每一个 $\lambda_i, \mu_i \in \{0, g, g^2, \dots, g^{q-1}\}$ 的 $i \in \{k, k+1, \dots, n-1\}$ 都意味着对于每一个 $i \in \{k, k+1, \dots, n-1\}$ 都有 $\lambda_i = \mu_i$ 。由于 $(\lambda_k - \mu_k)x_k \in J^{k+1}$ 和 $x_k \notin J^{k+1}$ ，我们有要么 $\lambda_k = \mu_k = 0$ 或者 $\lambda_k = g_k^\alpha$ 和 $\mu_k = g_k^\beta$ 对于某些 $\alpha_k, \beta_k \in \{0, 1, \dots, q-1\}$ 。由元素 g 的性质可知这蕴含了 $\alpha_k = \beta_k$ ，所以 $\lambda_k = \mu_k$ 。现在，假设对于所有的 $i = k, k+1, \dots, j$ 都有 $\lambda_i = \mu_i$ 。然后方程 (1) 给出了 $\sum_{i=j+1}^{n-1} \lambda_i x_i = \sum_{i=j+1}^{n-1} \mu_i x_i$ ，我们可以使用上述相同的论点来证明 $\lambda_{j+1} = \mu_{j+1}$ 。由于 $|J^k| = q^{n-k}$ ，我们看到 $J^k = X_k$ 。类似的论证也给出了 $J^k = Y_k = \{\sum_{i=k}^{n-1} x_i \mu_i; \mu_i \in \{0, g, g^2, \dots, g^{q-1}\} \text{ for every } i \in \{k, k+1, \dots, n-1\}\}$ 。由于 $x_1 g \in J \setminus J^2$ ，我们看到对于某个 $\alpha \in \{0, 1, \dots, q-1\}$ 和某个 $j \in J^2$ 有 $x_1 g = g^\alpha x_1 + j$ 。 $J = X_1$ 、 $J^n = 0$ 和 $J^{n-1} \neq 0$ 现在表明 $x_1^{n-1} \neq 0$ ，因此对于每一个 $i = 1, 2, \dots, n-1$ 都有 $x_1^i \in J^i \setminus J^{i+1}$ 。现在，任选一个 $x \in J^k \setminus J^{k+1}$ 。根据上述内容，我们有 $x = \sum_{i=k}^{n-1} \lambda_i x_1^i$ 对于某个 $\lambda_i \in \{0, g, g^2, \dots, g^{q-1}\}$ 具有 $\lambda_k \neq 0$ 。同样选择任意的 $y = \sum_{i=k}^{n-1} x_1^i \mu_i \in J^k$ ，具有 $\mu_i \in \{0, g, g^2, \dots, g^{q-1}\}$ 。注意，由引理 4.5 可知 $x' = \sum_{i=k}^{n-1} \lambda_i x_1^{i-k} \in R^*$ ，因此 $xx'^{-1} = x_1^k$

并且进而 $xx'^{-1}(\sum_{i=k}^{n-1} x_1^{i-k} \mu_i) = y$ 。我们已经证明了 $xR = J^k$ 。由于 $xR \simeq R/\text{Ann}_r(x)$, 这意味着 $|\text{Ann}_r(x)| = q^k$, 并且因为 $J^{n-k} \subseteq \text{Ann}_r(x)$, 我们已经证明了 $\text{Ann}_r(x) = J^{n-k}$ 。选择 $a \in R$ 并注意 $\delta_x(a) = 0$ 当且仅当 $a \in J^{k+1}$ 。现在, 引理 2.3 给出了 $\text{Prob}_x(R) = \frac{\sum_{a \in R \setminus J^{k+1}} |\text{Ann}_r(a)|}{|R|^2} = \frac{\sum_{i=0}^k \sum_{a \in J^i \setminus J^{i+1}} |\text{Ann}_r(a)|}{|R|^2}$ 。对于任意的 $a \in J^i \setminus J^{i+1}$, 我们有 $\text{Ann}_r(a) = J^{n-i}$, 所以 $|\text{Ann}_r(a)| = q^i$ 。此外, $|J^i \setminus J^{i+1}| = q^{n-i} - q^{n-i-1}$, 这给出了 $\text{Prob}_x(R) = \frac{\sum_{i=0}^k q^{n-i}(q-1)}{|R|^2} = \frac{(k+1)(q-1)}{q^{n+1}}$ 。

最后, 如果 $x = 0$, 那么对于每一个 $a \in R$ 都有 $\delta_x(a) = 1$, 所以我们得到 $\text{Prob}_x(R) = \frac{|R| + \sum_{i=0}^{n-1} \sum_{a \in J^i \setminus J^{i+1}} |\text{Ann}_r(a)|}{|R|^2} = \frac{q^n + \sum_{i=0}^{n-1} q^{n-1}(q-1)}{q^{2n}} = \frac{q+n(q-1)}{q^{n+1}} = \frac{(n+1)q-n}{q^{n+1}}$ 。 ■

备注 1. 注意到定理 4.6 直接给出了任何 $x \in R$ 的 $\text{Prob}_x(R)$ 的具体值, 在 $R = \mathbb{Z}_{p^r}$ 的情况下, 对于某个整数 r 和素数 p 。然而, 来自 [21] 的定理 2.1 和 2.2 仅仅给出了求和公式。此外, 引理 4.6 和引理 2.5 现在也给出了 $\text{Prob}_x(R)$ 在 $R = \mathbb{Z}_n$ 情况下的一个公式, 适用于任意整数 n 和任意 $x \in R$, 这推广了来自 [18] 的定理 2.10、2.11、2.12、2.13、2.14 和 2.15。

我们还有以下定理。

定理 4.7. 令 R 是一个有限局部环, 并具有 $|R| = q^n$ 和 $R/J = GF(q)$, 并假设 $J^2 = 0$ 成立。那么 $\text{Prob}_x(R) = \begin{cases} \frac{2(q-1)}{q^{n+1}}, & \text{if } 0 \neq x \in J, \\ \frac{q-1}{q^{n+1}}, & \text{if } x \notin J, \\ \frac{q^{n-1}+2q-2}{q^{n+1}}, & \text{if } x = 0. \end{cases}$

Proof. 选择 $0 \neq x \in J$, 然后选择 $0 \neq a \in J$, 使得 $\delta_x(a) = 1$ 。由于 $J^2 = 0$, 如果存在 $b \in R$ 使得 $ab = x$, 我们知道 $b \notin J$, 所以 b 是可逆的, 从而 $a = xb^{-1}$ 。然而, 如果对于两个不同的可逆元素 b_1 和 b_2 有 $xb_1 = xb_2$, 则 $x(b_1 - b_2) = 0$, 所以 $b_1 - b_2 \in J$, 因此至少存在 $q-1$ 个不同形式的非零元素 xb , 其中一些可逆元素为 $b \in R$ 。由于 $J^2 = 0$, 我们有 $|xR \setminus \{0\}| = q-1$, 因此我们恰好有 $q-1$ 个不同的元素 $a \in J$ 满足 $\delta_x(a) = 1$ 。对于每个这样的 a , 我们有 $\text{Ann}_r(a) = J$ 。另一方面, 如果 $a \notin J$, 则 a 是可逆的, 因此 $\delta_x(a) = 1$ 和 $\text{Ann}_r(a) = \{0\}$ 。因此根据引理 2.3, 我们有 $\text{Prob}_x(R) = \frac{(q-1)|J| + |R^*|}{|R|^2} = \frac{2(q-1)q^{n-1}}{q^{2n}} = \frac{2(q-1)}{q^{n+1}}$ 。如果 $x \notin J$, 我们由定理 4.2 得到 $\text{Prob}_x(R) = \frac{q-1}{q^{n+1}}$ 。最后, 如果 $x = 0$, 我们有 $|\text{Ann}_r(a)| = 1$ 对于可逆元素 a , $|\text{Ann}_r(a)| = q^{n-1}$ 对于不可逆非零元素 a 以及当然 $|\text{Ann}_r(0)| = q^n$, 所以 $\text{Prob}_x(R) = \frac{q^{n-1}(q-1) + (q^{n-1}-1)q^{n-1} + q^n}{q^{2n}} = \frac{q^{n-1}+2q-2}{q^{n+1}}$ 。 ■

致谢

作者感谢匿名审稿人提供了有用且详细的评论, 这些评论有助于提高本文的质量。

声明与陈述

作者声明没有利益冲突。

REFERENCES

1. George E. Andrews, *The theory of partitions*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998, Reprint of the 1976 original. MR 1634067
2. F. Barry, D. MacHale, and Á. Ní Shé, *Some supersolvability conditions for finite groups*, Math. Proc. R. Ir. Acad. **106A** (2006), no. 2, 163–177. MR 2266824
3. Dhiren Kumar Basnet and Jutirekha Dutta, *Some bounds for commuting probability of finite rings*, Proc. Indian Acad. Sci. Math. Sci. **129** (2019), no. 1, Paper No. 1, 6. MR 3887207
4. S. M. Buckley, D. MacHale, and Y. Zelenyuk, *Finite rings with large anticommuting probability*, Appl. Math. Inf. Sci. **8** (2014), no. 1, 13–25. MR 3117772
5. Stephen M. Buckley and Desmond MacHale, *Commuting probability for subrings and quotient rings*, J. Algebra Comb. Discrete Struct. Appl. **4** (2017), no. 2, 189–196. MR 3601350
6. David Dolžan, *The probability of zero multiplication in finite rings*, Bull. Aust. Math. Soc. **106** (2022), no. 1, 83–88. MR 4448946
7. Jutirekha Dutta, Dhiren Kumar Basnet, and Rajat Kanti Nath, *On commuting probability of finite rings*, Indag. Math. (N.S.) **28** (2017), no. 2, 372–382. MR 3624561
8. ———, *Characterization and commuting probability of n -centralizer finite rings*, Proyecciones **42** (2023), no. 6, 1489–1498. MR 4679483
9. M. A. Esmkhani and S. M. Jafarian Amiri, *The probability that the multiplication of two ring elements is zero*, J. Algebra Appl. **17** (2018), no. 3, 1850054, 9. MR 3760023
10. ———, *Characterization of rings with nullity degree at least $\frac{1}{4}$* , J. Algebra Appl. **18** (2019), no. 4, 1950076, 8. MR 3928520
11. Robert M. Guralnick and Geoffrey R. Robinson, *On the commuting probability in finite groups*, J. Algebra **300** (2006), no. 2, 509–528. MR 2228209
12. W. H. Gustafson, *What is the probability that two group elements commute?*, Amer. Math. Monthly **80** (1973), 1031–1034. MR 327901
13. Yuji Kobayashi and Kwangil Koh, *A classification of finite rings by zero divisors*, J. Pure Appl. Algebra **40** (1986), no. 2, 135–147. MR 830317
14. Paul Lescot, *Isoclinism classes and commutativity degrees of finite groups*, J. Algebra **177** (1995), no. 3, 847–869. MR 1358488
15. Desmond MacHale, *Commutativity in finite rings*, Amer. Math. Monthly **83** (1975), no. 1, 30–32. MR 384861
16. Haval M. Mohammed Salih, *On the probability of zero divisor elements in group rings*, Int. J. Group Theory **11** (2022), no. 4, 253–257. MR 4509600
17. R. Raghavendran, *Finite associative rings*, Compositio Math. **21** (1969), 195–229. MR 246905
18. Shafiq ur Rehman and Muhammad Naveed Shaheryar, *On generalized probability in finite commutative rings*, Int. Electron. J. Algebra **33** (2023), 125–132. MR 4563792
19. David J. Rusin, *What is the probability that two elements of a finite group commute?*, Pacific J. Math. **82** (1979), no. 1, 237–247. MR 549847

20. Pavel Shumyatsky and Matteo Vannacci, *Commuting and product-zero probability in finite rings*, Internat. J. Algebra Comput. **34** (2024), no. 2, 201–206. MR 4727826
21. Shafiq ur Rehman, Abdul Qudair Baig, and Kamran Haider, *A probabilistic approach toward finite commutative rings*, Southeast Asian Bull. Math. **43** (2019), no. 3, 413–418. MR 3966299

D. DOLŽAN: DEPARTMENT OF MATHEMATICS, FACULTY OF MATHEMATICS AND PHYSICS, UNIVERSITY OF LJUBLJANA, JADRANSKA 19, SI-1000 LJUBLJANA, SLOVENIA, AND INSTITUTE OF MATHEMATICS, PHYSICS AND MECHANICS, JADRANSKA 19, SI-1000 LJUBLJANA, SLOVENIA; E-MAIL: DAVID.DOLZAN@FMF.UNI-LJ.SI