Erdős-Burgess constant of the multiplicative semigroup of the quotient ring of $\mathbb{F}_q[x]$

Jun Hao\textsuperscript{a} Haoli Wang\textsuperscript{b,*} Lizhen Zhang\textsuperscript{a}

\textsuperscript{a}Department of Mathematics, Tianjin Polytechnic University, Tianjin, 300387, P. R. China
\textsuperscript{b} College of Computer and Information Engineering
Tianjin Normal University, Tianjin, 300387, P. R. China

Abstract

Let $S$ be a semigroup endowed with a binary associative operation $\ast$. An element $e$ of $S$ is said to be idempotent if $e \ast e = e$. The Erdős-Burgess constant of the semigroup $S$ is defined as the smallest $\ell \in \mathbb{N} \cup \{\infty\}$ such that any sequence $T$ of terms from $S$ and of length $\ell$ contains a nonempty subsequence the product of whose terms, in some order, is idempotent. Let $q$ be a prime power, and let $\mathbb{F}_q[x]$ be the ring of polynomials over the finite field $\mathbb{F}_q$. Let $R = \mathbb{F}_q[x]/K$ be a quotient ring of $\mathbb{F}_q[x]$ modulo any ideal $K$. We gave a sharp lower bound of the Erdős-Burgess constant of the multiplicative semigroup of the ring $R$, in particular, we determined the Erdős-Burgess constant in the case when $K$ is factored into either a power of some prime ideal or a product of some pairwise distinct prime ideals in $\mathbb{F}_q[x]$.

Key Words: Erdős-Burgess constant; Davenport constant; Multiplicative semigroups; Polynomial rings

\textsuperscript{*}Corresponding author’s Email: bjpeuwanghaoli@163.com
1 Introduction

Let $S$ be a nonempty semigroup, endowed with a binary associative operation $*$ on $S$, and denote by $E(S)$ the set of idempotents of $S$, where $x \in S$ is said to be an idempotent if $x*x = x$.

P. Erdős posed a question on idempotent to D.A. Burgess as follows.

“If $S$ is a finite nonempty semigroup of order $n$, does any $S$-valued sequence $T$ of length $n$ contain a nonempty subsequence the product of whose terms, in some order, is an idempotent?”

In 1969, Burgess [1] answered this question in the case when $S$ is commutative or contains only one idempotent. This question was completely affirmed by D.W.H. Gillam, T.E. Hall and N.H. Williams, who proved the following stronger result:

**Theorem A.** ([2]) Let $S$ be a finite nonempty semigroup. Any $S$-valued sequence of length $|S| - |E(S)| + 1$ contains one or more terms whose product (in the order induced from the sequence $T$) is an idempotent; In addition, the bound $|S| - |E(S)| + 1$ is optimal.

G.Q. Wang [6] generalized the result in the context of arbitrary semigroups (including both finite and infinite semigroups).

**Theorem B.** ([6], Theorem 1.1) Let $S$ be a nonempty semigroup such that $|S \setminus E(S)|$ is finite. Any sequence $T$ of terms from $S$ of length $|T| \geq |S \setminus E(S)| + 1$ contains one or more terms whose product (in the order induced from the sequence $T$) is an idempotent.

Moreover, Wang [6] characterized the structure of extremal sequences of length $|S \setminus E(S)|$ and remarked that although the bound $|S \setminus E(S)| + 1$ is optimal for general semigroups $S$, the better bound can be obtained for specific classes of semigroups. Hence, Wang proposed two combinatorial additive constants associated with idempotents.

**Definition C.** ([6], Definition 4.1) Let $S$ be a nonempty semigroup and $T$ a sequence of terms from $S$. We say that $T$ is an idempotent-product sequence if its terms can be ordered so that their product is an idempotent element of $S$. We call $T$ (weakly) idempotent-product free if $T$ contains no nonempty idempotent-product subsequence, and we call $T$ strongly idempotent-product free if $T$ contains no nonempty subsequence the product whose terms, in the order induced from the sequence $T$, is an idempotent. We define $I(S)$, which is called the Erdős-Burgess constant of the semigroup $S$, to be the least $\ell \in \mathbb{N} \cup \{\infty\}$ such that every sequence $T$ of terms from $S$ of length at least $\ell$ is not (weakly) idempotent-product free, and we define $SI(S)$, which is called the strong Erdős-Burgess constant of the semigroup $S$, to be the least $\ell \in \mathbb{N} \cup \{\infty\}$ such that every sequence $T$ of terms from $S$ of length at least $\ell$ is not strongly...
idempotent-product free. Formally, one can also define

\[ I(S) = \sup \{|T| + 1 : T \text{ takes all idempotent-product free sequences of terms from } S \} \]

and

\[ SI(S) = \sup \{|T|+1 : T \text{ takes every strongly idempotent-product free sequences of terms from } S \} \]

Very recently, Wang [7] made a comprehensive study of the Erdős-Burgess constant for the direct product of arbitrarily many of cyclic semigroups. As pointed out in [6], the Erdős-Burgess constant reduces to be the famous Davenport constant in the case when the underlying semigroup happens to be a finite abelian group. So we need to introduce the definition of Davenport constant below.

Let \( G \) be an additive finite abelian group. A sequence \( T \) of terms from \( G \) is called a zero-sum sequence if the sum of all terms of \( T \) equals to zero, the identity element of \( G \). We call \( T \) a zero-sum free sequence if \( T \) contains no nonempty zero-sum subsequence. The Davenport constant \( D(G) \) of \( G \) is defined to be the smallest positive integer \( \ell \) such that, every sequence \( T \) of terms from \( G \) and of length at least \( \ell \) is not zero-sum free.

In 2008, Wang and Gao [8] extended the definition of the Davenport constant to commutative semigroups as follows.

**Definition D.** Let \( S \) be a finite commutative semigroup. Let \( T \) be a sequence of terms from the semigroup \( S \). We call \( T \) reducible if \( T \) contains a proper subsequence \( T' \) (\( T' \neq T \)) such that the sum of all terms of \( T' \) equals the sum of all terms of \( T \). Define the Davenport constant of the semigroup \( S \), denoted \( D(S) \), to be the smallest \( \ell \in \mathbb{N} \cup \{\infty\} \) such that every sequence \( T \) of length at least \( \ell \) of terms from \( S \) is reducible.

Several related additive results on Davenport constant for semigroups were obtained (see [4], [5], [9], [10]). For any commutative ring \( R \), we denote \( S_R \) to be the multiplicative semigroup of the ring \( R \) and \( U(S_R) \) to be the group of units of the semigroup \( S_R \). With respect to the Davenport constant for the multiplicative semigroup associated with polynomial rings \( \mathbb{F}_q[x] \), Wang obtained the following result.

**Theorem E.** ([4]) Let \( q > 2 \) be a prime power, and let \( \mathbb{F}_q[x] \) be the ring of polynomials over the finite field \( \mathbb{F}_q \). Let \( R \) be a quotient ring of \( \mathbb{F}_q[x] \) with \( 0 \neq R \neq \mathbb{F}_q[x] \). Then \( D(S_R) = D(U(S_R)) \).

G.Q. Wang [4] proposed to determine \( D(S_R) - D(U(S_R)) \) for the remaining case that \( R \) is a quotient ring of \( \mathbb{F}_2[x] \).
L.Z. Zhang, H.L. Wang and Y.K. Qu partially answered Wang’s question and obtained the following.

**Theorem F.** ([10]) Let \( \mathbb{F}_2[x] \) be the ring of polynomials over the finite field \( \mathbb{F}_2 \), and let \( R = \mathbb{F}_2[x]/(f) \) be a quotient ring of \( \mathbb{F}_2[x] \), where \( f \in \mathbb{F}_2[x] \) and \( 0 \neq R \neq \mathbb{F}_2[x] \). Then

\[
D(U(S_R)) \leq D(S_R) \leq D(U(S_R)) + \delta_f,
\]

where

\[
\delta_f = \begin{cases} 
0 & \text{if } \gcd(x \ast (x + 1_{\mathbb{F}_2}), f) = 1_{\mathbb{F}_2}; \\
1 & \text{if } \gcd(x \ast (x + 1_{\mathbb{F}_2}), f) \in \{x, x + 1_{\mathbb{F}_2}\}; \\
2 & \text{if } \gcd(x \ast (x + 1_{\mathbb{F}_2}), f) = x \ast (x + 1_{\mathbb{F}_2}).
\end{cases}
\]

Motivated by the above additive research on semigroups, in this manuscript we make a study of the Erdős-Burgess constant on the multiplicative semigroups of the quotient rings of the polynomial rings \( \mathbb{F}_q[x] \) and obtain the following result.

**Theorem 1.1.** Let \( q \) be a prime power, and let \( \mathbb{F}_q[x] \) be the ring of polynomials over the finite field \( \mathbb{F}_q \). Let \( R = \mathbb{F}_q[x]/K \) be a quotient ring of \( \mathbb{F}_q[x] \) modulo any ideal \( K \). Then

\[
I(S_R) \geq D(U(S_R)) + \Omega(K) - \omega(K),
\]

where \( \Omega(K) \) is the number of the prime ideals (repetitions are counted) and \( \omega(K) \) the number of distinct prime ideals in the factorization when \( K \) is factored into a product of prime ideals. Moreover, the equality holds for the case when \( K \) is factored into either a power of some prime ideal or a product of some pairwise distinct prime ideals in \( \mathbb{F}_q[x] \).

## 2 Notation

Let \( S \) be a finite commutative semigroup. The operation on \( S \) will be denoted by \( + \) instead of \( \ast \). The identity element of \( S \), denoted \( 0_S \) (if exists), is the unique element \( e \) of \( S \) such that \( e + a = a \) for every \( a \in S \). If \( S \) has an identity element \( 0_S \), let

\[
U(S) = \{a \in S : a + a' = 0_S \text{ for some } a' \in S\}
\]

be the group of units of \( S \). The sequence \( T \) of terms from the semigroups \( S \) is denoted by

\[
T = a_1a_2 \cdot \ldots \cdot a_\ell = \bigcap_{a \in S} a_{v_a(T)},
\]
where \( v_a(T) \) denotes the multiplicity of the element \( a \) occurring in the sequence \( T \). By \( \cdot \) we denote the operation to join sequences. Let \( T_1, T_2 \) be two sequences of terms from the semigroups \( S \). We call \( T_2 \) a subsequence of \( T_1 \) if

\[
v_a(T_2) \leq v_a(T_1)
\]

for every element \( a \in S \), denoted by

\[
T_2 \mid T_1.
\]

In particular, if \( T_2 \neq T_1 \), we call \( T_2 \) a proper subsequence of \( T_1 \), and write

\[
T_3 = T_1 T_2^{-1}
\]

to mean the unique subsequence of \( T_1 \) with \( T_2 \cdot T_3 = T_1 \). Let

\[
\sigma(T) = a_1 + a_2 + \cdots + a_\ell
\]

be the sum of all terms in the sequence \( T \).

Let \( q \) be a prime power, and let \( \mathbb{F}_q[x] \) be the ring of polynomials over the finite field \( \mathbb{F}_q \). Let \( R = \mathbb{F}_q[x] / K \) be the quotient ring of \( \mathbb{F}_q[x] \) modulo the ideal \( K \), and let \( S_R \) be the multiplicative semigroup of the ring \( R \). Take an arbitrary element \( a \in S_R \). Let \( \theta_a \in \mathbb{F}_q[x] \) be the unique polynomial corresponding to the element \( a \) with the least degree, thus, \( \theta_a = \theta_a + K \) is the corresponding form of \( a \) in the quotient ring \( R \).

\( \bullet \) In what follows, since we deal with only the multiplicative semigroup \( S_R \) which happens to be commutative, we shall use the terminology idempotent-sum and idempotent-sum free in place of idempotent-product and idempotent-product free, respectively.

### 3 Proof of Theorem 1.1

**Lemma 3.1.** Let \( q \) be a prime power, and let \( \mathbb{F}_q[x] \) be the ring of polynomials over the finite field \( \mathbb{F}_q \). Let \( f \) be a polynomial in \( \mathbb{F}_q[x] \) and let \( f = p_{r_1}^{n_1} p_{r_2}^{n_2} \cdots p_{r_r}^{n_r} \), where \( r \geq 1, n_1, n_2, \ldots, n_r \geq 1 \), and \( p_1, p_2, \ldots, p_r \) are pairwise non-associate irreducible polynomials in \( \mathbb{F}_q[x] \). Let \( R = \mathbb{F}_q[x] / (f) \) be the quotient ring of \( \mathbb{F}_q[x] \) modulo the ideal \( (f) \). Let \( a \) be an element in the semigroup of \( S_R \). Then \( a \) is idempotent if and only if \( \theta_a \equiv 0_{\mathbb{F}_q} (\mod p_i^{n_i}) \) or \( \theta_a \equiv 1_{\mathbb{F}_q} (\mod p_i^{n_i}) \) for every \( i \in [1, r] \).
Proof. Suppose that \(a\) is idempotent. Then \(\theta_a \equiv \theta_a \pmod{f}\), which implies that \(\theta_a(\theta_a - 1) \equiv 0 \pmod{f}\) for all \(i \in [1, r]\). Since \(\gcd(\theta_a, \theta_a - 1) = 1\), it follows that for every \(i \in [1, r]\), \(p_i^{n_i}\) divides \(\theta_a\) or \(p_i^{n_i}\) divides \(\theta_a - 1\), that is, \(\theta_a \equiv 0 \pmod{p_i^{n_i}}\) or \(\theta_a \equiv 1 \pmod{p_i^{n_i}}\). Then the necessity holds. The sufficiency holds similarly. □

We remark that in Theorem 1.1, if \(K = \mathbb{F}_q[x]\), then \(R\) is a trivial zero ring and \(I(S_R) = D(S_R) = 1\) and \(\Omega(K) = \omega(K) = 0\), and if \(K\) is the zero ideal then \(R = \mathbb{F}_q[x]\) and \(I(S_R)\) is infinite since any sequence \(T\) of any length such that \(\theta_a\) is a nonconstant polynomial for all terms \(a\) of \(T\) is an idempotent-sum free sequence, and thus, the conclusion holds trivially for both cases. Hence, we shall only consider the case that \(K\) is nonzero proper ideal of \(\mathbb{F}_q[x]\) in what follows.

Proof of Theorem 1.1. Note that \(\mathbb{F}_q[x]\) is a principal ideal domain. Say

\[K = (f)\]

is the principal ideal generated by a polynomial \(f \in \mathbb{F}_q[x]\), where

\[f = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},\]

where \(p_1, p_2, \ldots, p_r\) are pairwise non-associate irreducible polynomials of \(\mathbb{F}_q[x]\) and \(n_i \geq 1\) for all \(i \in [1, r]\), equivalently,

\[K = P_1^{n_1} P_2^{n_2} \cdots P_r^{n_r}\]

is the factorization of the ideal \(K\) into the product of the powers of distinct prime ideals \(P_1 = (p_1), P_2 = (p_2), \ldots, P_r = (p_r)\). Observe that

\[\Omega(K) = \sum_{i=1}^{r} n_i\]

and

\[\omega(K) = r.\]

Take a zero-sum free sequence \(V\) of terms from the group \(U(S_R)\) of length \(D(U(S_R)) - 1\). Take \(b_i \in S_R\) such that \(\theta_{b_i} = p_i\) for each \(i \in [1, r]\). Now we show that the sequence \(V \cdot \prod_{i=1}^{r} b_i^{n_i-1}\) is an idempotent-sum free sequence in \(S_R\). Suppose to the contrary that \(V \cdot \prod_{i=1}^{r} b_i^{n_i-1}\) contains a nonempty subsequence \(W\), say \(W = V' \cdot \prod_{i=1}^{r} b_i^{\beta_i}\), such that \(\sigma(W)\) is idempotent, where \(V'\) is a subsequence of \(V\) and \(\beta_i \in [0, n_i - 1]\) for all \(i \in [1, r]\).
It follows that
\[ \theta_{\sigma(W)} = \theta_{\sigma(V') \sigma_i(1)} \theta_{\sigma_i(b_i)} = \theta_{\sigma(V')} p_1^{\beta_1} \cdots p_r^{\beta_r}. \]  

(5)

If \( \sum_{i=1}^{r} \beta_i = 0 \), then \( W = V' \) is a nonempty subsequence of \( V \). Since \( V \) is zero-sum free in the group of \( U(S_R) \), we derive that \( \sigma(W) \) is a nonidentity element of the group \( U(S_R) \), and thus, \( \sigma(W) \) is not idempotent, a contradiction. Otherwise, \( \beta_j > 0 \) for some \( j \in [1, r] \), say

\[ \beta_1 \in [1, n_1 - 1]. \]  

(6)

Since \( \gcd(\theta_{\sigma(V')}, p_1) = 1 \), it follows from (5) that \( \gcd(\theta_{\sigma(W)}, p_1^{\beta_1}) = p_1^{\beta_1} \). Combined with (6), we have that \( \theta_{\sigma(W)} \not\equiv 0 \pmod{p_1^{\beta_1}} \) and \( \theta_{\sigma(W)} \not\equiv 1 \pmod{p_1^{\beta_1}} \). By Lemma 5.1, we conclude that \( \sigma(W) \) is not idempotent, a contradiction. This proves that the sequence \( V \cdot \prod_{i=1}^{r} b_i^{n_i-1} \) is idempotent-sum free in \( S_R \). Combined with (3) and (4), we have that

\[ I(S_R) \geq |V| \sum_{i=1}^{r} b_i^{n_i-1} + 1 = (|V| + 1) + \sum_{i=1}^{r} (n_i - 1) = D(U(S_R)) + \Omega(K) - \omega(K). \]  

(7)

Now we assume that \( K \) is factored into either a power of some prime ideal or a product of some pairwise distinct prime ideals in \( \mathbb{F}_q[x] \), i.e., either \( r = 1 \) or \( n_1 = \cdots = n_r = 1 \) in (2).

It remains to show the equality \( I(S_R) = D(U(S_R)) + \Omega(K) - \omega(K) \) holds. We distinguish two cases.

**Case 1.** \( r = 1 \) in (2), i.e., \( f = p_1^{n_1} \).

Take an arbitrary sequence \( T \) of length \( |T| = D(U(S_R)) + n_1 - 1 = D(U(S_R)) + \Omega(K) - \omega(K) \). Let \( T_1 = \prod_{i=0}^{\theta_i \equiv 0 \pmod{p_1}} a \) and \( T_2 = TT_1^{-1} \). Note that all terms of \( T_2 \) are from \( U(S_R) \). By the Pigeonhole Principle, we see that either \( |T_1| \geq n_1 \) or \( |T_2| \geq D(U(S_R)) \). It follows that either \( \theta_{\sigma(T_1)} \equiv 0 \pmod{p_1^{n_1}} \), or \( T_2 \) contains a nonempty subsequence \( T'_2 \) such that \( \sigma(T'_2) \) is the identity element of the group \( U(S_R) \). By Lemma 5.1, the sequence \( T \) is not idempotent-sum free, which implies that \( I(S_R) \leq D(U(S_R)) + \Omega(K) - \omega(K) \). Combined with (7), we have that

\[ I(S_R) = D(U(S_R)) + \Omega(K) - \omega(K). \]

**Case 2.** \( n_1 = \cdots = n_r = 1 \) in (2), i.e., \( f = p_1 p_2 \cdots p_r \).

Then

\[ \Omega(K) = \omega(K) = r. \]  

(8)
Take an arbitrary sequence $T$ of length $|T| = D(U(S_R))$. For any term $a$ of $T$, let $\tilde{a} \in S_R$ be such that for each $i \in [1, r]$,

$$\theta_a \equiv \begin{cases} 1_{F_q} \pmod{p_i} & \text{if } \theta_a \equiv 0_{F_q} \pmod{p_i}; \\ \theta_a \pmod{p_i} & \text{otherwise.} \end{cases} \tag{9}$$

Note that $\tilde{a} \in U(S_R)$.

Let $\tilde{T} = \bigsqcup_{a \in T} \tilde{a}$. Then $\tilde{T}$ is a sequence of terms from the group $U(S_R)$ with length $|\tilde{T}| = |T| = D(U(S_R))$. It follows that there exists a nonempty subsequence $W$ of $T$ such that $\sigma(\bigsqcup_{a \in W} \tilde{a})$ is the identity element of the group $U(S_R)$, i.e., $\theta_{\sigma(\bigsqcup_{a \in W} \tilde{a})} = 1_{F_q} \pmod{p_i}$ for each $i \in [1, r]$. By (9), we derive that $\theta_{\sigma(W)} \equiv 0_{F_q} \pmod{p_i}$ or $\theta_{\sigma(W)} \equiv 1_{F_q} \pmod{p_i}$ for each $i \in [1, r]$. By Lemma 3.1, we conclude that $\sigma(W)$ is idempotent. Combined with (8), we have that $I(S_R) \leq D(U(S_R)) = D(U(S_R)) + \Omega(K) - \omega(K)$. It follows from (7) that $I(S_R) = D(U(S_R)) + \Omega(K) - \omega(K)$, completing the proof. \hfill \Box

We close this paper with the following conjecture.

**Conjecture 3.2.** Let $q > 2$ be a prime power, and let $\mathbb{F}_q[x]$ be the ring of polynomials over the finite field $\mathbb{F}_q$. Let $R = \mathbb{F}_q[x]/K$ be a quotient ring of $\mathbb{F}_q[x]$ modulo any nonzero proper ideal $K$. Then $I(S_R) = D(U(S_R)) + \Omega(K) - \omega(K)$.

Acknowledgements

This work is supported by NSFC (grant no. 11501561, 61303023).

References

[1] D.A. Burgess, *A problem on semi-groups*, Studia Sci. Math. Hungar., 4 (1969) 9–11.

[2] D.W.H. Gillam, T.E. Hall and N.H. Williams, *On finite semigroups and idempotents*, Bull. Lond. Math. Soc., 4 (1972) 143–144.

[3] K. Rogers, *A Combinatorial problem in Abelian groups*, Proc. Cambridge Phil. Soc., 59 (1963) 559–562.

[4] G.Q. Wang, *Davenport constant for semigroups II*, J. Number Theory, 153 (2015) 124–134.
[5] G.Q. Wang, *Additively irreducible sequences in commutative semigroups*, J. Combin. Theory Ser. A, **152** (2017) 380–397.

[6] G.Q. Wang, *Structure of the largest idempotent-free sequences in finite semigroups*, arXiv:1405.6278.

[7] G.Q. Wang, *Erdős-Burgess constant of the direct product of cyclic semigroups*, arXiv:1802.08791.

[8] G.Q. Wang and W.D. Gao, *Davenport constant for semigroups*, Semigroup Forum, **76** (2008) 234–238.

[9] G.Q. Wang and W.D. Gao, Davenport constant of the multiplicative semigroup of the ring $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$, arXiv:1603.06030.

[10] L.Z. Zhang, H.L. Wang and Y.K. Qu, *A problem of Wang on Davenport constant for the multiplicative semigroup of the quotient ring of $\mathbb{F}_2[x]$*, Colloq. Math., **148** (2017) 123–130.