ASYMPTOTIC FOR THE NUMBER OF STAR OPERATIONS ON ONE-DIMENSIONAL NOETHERIAN DOMAINS

Dario Spirito

Abstract. We study the set of star operations on local Noetherian domains $D$ of dimension 1 such that the conductor $(D : T)$ (where $T$ is the integral closure of $D$) is equal to the maximal ideal of $D$. We reduce this problem to the study of a class of closure operations (more precisely, multiplicative operations) in a finite extension $k \subseteq B$, where $k$ is a field, and then we study how the cardinality of this set of closures vary as the size of $k$ varies while the structure of $B$ remains fixed.

1. Introduction

Star operations are a class of closure operations on the set of (fractional) ideals of an integral domain that has been first studied by Krull [12] and Gilmer [4, Chapter 5]. Along the years, they have been used, for example, to study and generalize factorization properties (for example, with the characterization of unique factorization domains among Krull domain through the $t$-class group by Samuel [16]) and to find Prüfer-like classes of integral domains (for example PrMDs; see for example [1, Section 3] for an overview).

More recently, Houston, Mimouni and Park have been studying the set $\text{Star}(D)$ of star operations on an integral domain $D$, attempting to characterize when this set is finite and, in this case, to calculate its cardinality [7–10]. They analyzed in particular the Noetherian case, showing that $|\text{Star}(D)| = \infty$ when $D$ has dimension greater than 1 [8, Theorem 2.1], showing how to reduce to the local case [8, Theorem 2.3] and calculating the cardinality of $\text{Star}(D)$ when $\ell_D(T/m_D) \leq 3$, where $T$ is the integral closure of $D$ and $m_D$ the maximal ideal of $D$ [8, Theorem 3.1]. Further cases have been considered, for example, in [8] (for infinite residue field), in [15, 18] (for pseudo-valuation domains), in [17] (for Kunz domains) and [22] (for some numerical semigroup rings).

Beyond star operations, there are two other classes of closure operations that are in use in commutative algebra: semiprime operations, defined on the set of integral ideals of an arbitrary ring, and semistar operations, defined on the set
of all submodules of the quotient field of an integral domain. There are several
connections between the classes of semiprime, star and semistar operations; indeed, most definitions and many properties can be stated in essentially the
same way, with the main difference being often in how they must be phrased to
account for the different partially ordered set on which the closures are defined.

To unify the treatment of these classes of closure operations, the paper [20]
introduced the concept of multiplicative operations; these are a class of closure
operations that can be defined in any ring extension $A \subseteq B$ over any set $\mathcal{G}$ of
$A$-submodules of $B$, and their definition is flexible enough to cover (for suitable
choices of $A$, $B$ and $\mathcal{G}$) all three classical cases. Furthermore, multiplicative
operations enjoy some functorial properties; while these are usually a staple
of many semiprime operations, for star and semistar operations they are very
rare, especially due to the fact that quotienting an integral domain disrupts
its quotient field. (There are some limited exceptions; see [3] for properties of
star operations along pullbacks and [19] for an application to Prüfer domains.)

In the special case of local Noetherian domains of dimension 1, multiplicative
operations allow to bypass this problem by considering only the submodules
contained in the integral closure $T$ of the starting domain $D$ (which contain all
the needed data), and then by quotienting $T$ over the conductor $(D : T)$ (see
[20, Section 6] and the discussion after Definition 3.4 below). In particular,
this reduces the problem of finding all star operations on $D$ to the study of the
Artinian ring $T/(D : T)$.

In this paper, we continue the study initiated in Sections 6 and 7 of [20] on
this case, in particular concentrating on the case where the conductor $(D : T)$
is equal to the maximal ideal $m_D$ of $D$; in the Artinian setting, this case cor-
respond to the study of a particular set of multiplicative operations defined on
a finite extension $k \subseteq B$, where $k$ is a field. As we are interested in cardinality
problems, we assume throughout the paper that $k$ is a finite field of cardinality
$q$: in particular, we are interested in what happens when the structure of $B$ is
“fixed” (see Section 3 for a more precise definition) while $q$ changes, that is, we
are interested in the cardinality of the set $\text{Star}(D)$ of star operations on $D$ as a
function of $q$, and especially in understanding how fast the growth of $|\text{Star}(D)|$
is.

The aim of this paper is to introduce and give some evidence to the following
conjecture: if the structure of $B$ is fixed, then the function

$$q \mapsto \log_q \log_2 |\text{Star}(D)|$$

has always a limit as $q \to \infty$, and this limit depends only on the length of
$B = T/m_D$ as a $D$-module. While we are not able to prove this conjecture
in full generality, we show polynomial bounds on the upper and lower limits
(respectively, Theorem 4.2 and Proposition 5.8, summarized in Theorem 5.9)
and we prove the conjecture in full for $\ell_D(T/m_D) \leq 4$ (Proposition 3.9 and
Theorem 7.6).


2. Closure operations

Let \((\mathcal{P}, \leq)\) be a partially ordered set. A closure operation on \(\mathcal{P}\) is a map \(c : \mathcal{P} \rightarrow \mathcal{P}\) such that, for every \(x, y \in \mathcal{P}\):
- \(x \leq c(x)\);
- if \(x \leq y\), then \(c(x) \leq c(y)\);
- \(c(c(x)) = c(x)\).

If \(c, d\) are closure operations on \(\mathcal{P}\), we write \(c \leq d\) if \(c(x) \leq d(x)\) for every \(x \in \mathcal{P}\).

Any closure operation \(c\) is uniquely determined by the set \(\mathcal{P}^c := \{ x \in \mathcal{P} \mid c(x) = x \}\) of its fixed points, i.e., two closure operations \(c\) and \(d\) are equal if and only if \(\mathcal{P}^c = \mathcal{P}^d\). Furthermore, \(c \leq d\) if and only if \(\mathcal{P}^c \supseteq \mathcal{P}^d\).

3. Artinian rings

Throughout the paper, we shall denote by \(k\) the finite field of cardinality \(q\) and by \(B\) a finite \(k\)-algebra that is a principal ideal ring; we also write \(\mathbb{F}_{q^e}\) for the field of cardinality \(q^e\), i.e., for the extension of \(k\) of degree \(e\). In particular, \(\mathbb{F}_q = k\).

We can write \(B\) as a direct product \(B_1 \times \cdots \times B_t\), where each \(B_i\) is a local \(k\)-algebra; by [11, Theorem 8] \(B_i\) is isomorphic to \(\mathbb{F}_{q^{e_i}}[X]/(X^{f_i}) \cong \mathbb{F}_{q^{e_i}}[[X]]/(X^{f_i})\) for some positive integers \(e_i, f_i\). We will always consider \(k\) as a subring of \(B\) through the diagonal embedding; we shall also sometimes consider \(k\) as a subring of \(B_i\) by the obvious embedding of \(k\) into \(\mathbb{F}_{q^{e_i}}[X]/(X^{f_i})\).

It is easy to see that the quantities \(e_i, f_i\) are linked to the length of \(B\).

**Proposition 3.1.** Preserve the notation above. Then:
- \(f_i = \ell_{B_i}(B_i) = \ell_B(B_i)\);
- \(\mathbb{F}_{q^{e_i}}\) is the residue field of \(B_i\);
Proposition 3.3. \( \text{Preserve the notation above.} \)

Let \( s := \{ (e_1, f_1), \ldots, (e_r, f_r) \} \) be a sequence of pairs of positive integers. We call the ring
\[
B_s := \frac{\mathbb{F}_{q^r}[X]}{(X^{f_1})} \times \cdots \times \frac{\mathbb{F}_{q^r}[X]}{(X^{f_r})}
\]
the Artinian ring associated to \( s \). We denote by \( n(s) \) the sum \( \sum e_if_i = \ell_k(B_s) \).

Remark 3.2. The methods we will use actually hold in the more general setting of a ring extension \( A \subseteq B \), where \( A \) and \( B \) are Artinian rings and \( B \) is a finite \( A \)-module; the restriction to \( A = k \), however, allows to simplify the notation. Furthermore, many proofs do not really use the hypothesis that \( k \) is finite if not to guarantee that the quantities involved are finite.

Let now \( k, B \) as above. We define:
\begin{itemize}
  \item \( \mathcal{F}_0(k, B) := \{ I \in \mathbb{F}_k(B) \mid IB = B \} \);
  \item \( \mathcal{F}_{\text{reg}}(k, B) := \{ I \in \mathbb{F}_k(B) \mid I \text{ contains a regular element of } B \} \);
  \item \( \mathcal{F}_1(k, B) := \{ I \in \mathbb{F}_k(B) \mid 1 \in I \} \).
\end{itemize}

These sets are related in the following way.

Proposition 3.3. \( \text{Preserve the notation above.} \)

\begin{itemize}
  \item[(a)] \( \mathcal{F}_1(k, B) \subseteq \mathcal{F}_{\text{reg}}(k, B) \subseteq \mathcal{F}_0(k, B) \).
  \item[(b)] \( \text{If } |\text{Max}(B)| \leq q, \text{ then } \mathcal{F}_0(A, B) = \mathcal{F}_{\text{reg}}(A, B) \).
  \item[(c)] \( \text{If } \mathcal{F}_0(A, B) = \mathcal{F}_{\text{reg}}(A, B), \text{ then the restriction map from } \text{Mult}(k, B, \mathcal{F}_0(k, B)) \text{ to } \text{Mult}(k, B, \mathcal{F}_1(k, B)) \text{ is an order isomorphism.} \)
\end{itemize}

Proof. \((a)\) is obvious.

\((b)\) Let \( I \in \mathcal{F}_0(k, B) \). If \( I \) is not regular, then \( I \) is contained in the union of the maximal ideals of \( B \); by [8, Lemma 3.6], it follows that \( I \) is contained in some maximal ideal of \( B \). But this would imply \( 1 \notin IB \), a contradiction.

\((c)\) Let \( I \in \mathcal{F}_0(k, B) \). By hypothesis, \( I \) contains a regular element \( u \) of \( B \), which is a unit since \( B \) is Artinian; in particular, \( u^{-1}I = (I : u) \in \mathcal{F}_1(k, B) \subseteq \mathcal{F}_0(k, B) \). Hence, \( (u^{-1}I)^* \subseteq u^{-1}I^* \) for every multiplicative operation \( * \) on \((k, B, \mathcal{F}_0(k, B))\); since we can do the same with the unit \( v := u^{-1} \), it follows that \( (u^{-1}I)^* = u^{-1}I^* \). Hence, every \( * \in \text{Mult}(k, B, \mathcal{F}_0(k, B)) \) is uniquely determined by its action on \( \mathcal{F}_1(A, B) \), and so the restriction map is injective; furthermore, every \( * \in \text{Mult}(A, B, \mathcal{F}_1(A, B)) \) can be extended to \( \mathcal{F}_0(A, B) \) by setting \( I^* := u(u^{-1}I)^* \) when \( u \in I \), and thus the map is also surjective. \( \square \)

Note that the equality \( \mathcal{F}_0(k, B) = \mathcal{F}_{\text{reg}}(k, B) \) may indeed fail: for example, if \( k = \mathbb{F}_2 \) and \( B = k^3 \) the set \( V := \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\} \) is a \( k \)-module in \( \mathcal{F}_0(A, B) \), but it is not regular.

Definition 3.4. A \emph{star operation} on \((k, B)\) is a multiplicative operation \( * \) on \((k, B, \mathcal{F}_0(A, B))\) such that \( k^* = k \). We denote their set by \( \text{Star}(k, B) \).
The terminology is justified by the following situation: let \((D, m)\) be a Noetherian local integral domain of dimension 1, and let \(T\) be its integral closure. Suppose that \(T\) is finite over \(D\), and suppose that \((D : T) = m\). By [20, Theorem 6.4 and Corollary 6.5], there is an order-preserving bijection between the set of star operations on \(D\) and the set of star operations on \((D/m, T/m)\): in particular, \(\text{Star}(D)\) depends only on the extension \(k \subseteq T/m\) of Artinian rings, i.e., from the structure of the Artinian ring \(T/m\) as a \(k\)-algebra. Such a ring exists for every choice of \(s\), as the next proposition shows.

**Proposition 3.5.** Let \(s\) be a sequence of pairs of positive integers. Then, there is a local Noetherian domain \(D_s\) of dimension 1 with integral closure \(T\) such that \((D_s : T) = m\) and \(T/m \cong B_s\).

**Proof.** Let \(L_1, \ldots, L_t\) be the residue fields of \(B_s\) and, for every \(i\), let \(f_i(X) \in k[X]\) be an irreducible polynomial with splitting field \(L_i\). In the polynomial ring \(k[X_1, \ldots, X_t]\), let \(P_i\) be the prime ideal generated by \(f_i(X_i)\), and let \(S := k[X_1, \ldots, X_t] \setminus \bigcup_i P_i\). Then, \(T := S^{-1}[X_1, \ldots, X_t]\) is a principal ideal domain with \(t\) maximal ideals, \(P_1T, \ldots, P_tT\), such that the residue field of \(P_iT\) is \(L_i\).

Let \(I := P_1^{e_1} \cdots P_t^{e_t}\). Then, \(T/I\) is isomorphic to \(B_s\); if \(\pi\) is the quotient \(T \rightarrow B_s\), defining \(D_s := \pi^{-1}(k)\) we have the ring we were looking for. \(\square\)

Note that, while \(B_s\) can be defined in a “canonical” way, there is a lot more freedom in defining \(D_s\), since it may be possible to use a polynomial ring with fewer indeterminates (for example, if each \(L_i\) has a different degree, then it is sufficient to consider \(T\) as a localization of \(k[X]\)).

**Definition 3.6.** Let \(s\) be a sequence of pairs of positive integers. We denote by \(\Lambda(s, q)\) the cardinality of \(\text{Star}(k, B_s)\), where \(q := |k|\).

If \(s\) is fixed, we can expect the function \(q \mapsto \Lambda(s, q)\) to be increasing, since as \(q\) grows the ring \(B_s\) contains more and more subspaces and thus more and more closure operations. Indeed, this is exactly what happens for \(n(s) > 3\), while for \(n(s) \leq 3\) the map \(\Lambda(s, q)\) is constant (see [8] and the proof of Proposition 3.9 below). To study how fast it grows, we introduce the following function.

**Definition 3.7.** Let \(s\) be a sequence of pairs of positive integers. We set

\[
\theta(s, q) := \log_q \log_2 \Lambda(s, q).
\]

It is not at all obvious that this is a good choice. However, we have the following.

**Proposition 3.8.** For every \(n \in \mathbb{N}\), we have

\[
\lim_{q \to \infty} \theta((n, 1), q) = \begin{cases} \frac{(n-2)^2}{4} & \text{if } n \text{ is even}, \\ \frac{(n-1)(n-3)}{4} & \text{if } n \text{ is odd}. \end{cases}
\]

**Proof.** If \(s = \{(n, 1)\}\), the ring \(B := B_s\) is just the degree \(n\) extension of \(k\). Let \(\gamma_n\) be the number on the right hand side in the formula of the statement.
Suppose \( n \) is even. By [18, Theorem 3.7], for every \( \epsilon > 0 \) we have, for large \( q \),
\[
q^{\gamma_n} \leq \log_2 |\text{Star}(k, B)| \leq (1 + \epsilon)q^{\gamma_n};
\]
taking the logarithm in base \( q \) we have
\[
\gamma_n \leq \theta((n, 1), q) \leq \gamma_n + \log_q (1 + \epsilon)
\]
and the claim follows by taking the limit. If \( n \) is odd, instead of \( 1 + \epsilon \) we have \( 2 + \epsilon \), but the same reasoning applies. \( \square \)

Another case when we can calculate the limit of \( \theta(s, q) \) is for low \( n(s) \).

**Proposition 3.9.** Let \( s \) be a sequence of pairs of positive integers. Then:

1. if \( n(s) \leq 2 \), then \( \theta(s, q) = -\infty \) for every \( q \);
2. if \( n(s) = 3 \), then
\[
\lim_{q \to \infty} \theta(s, q) = 0.
\]

**Proof.** By Proposition 3.5, we can find a local Noetherian domain \((D, \mathfrak{m})\) of dimension 1 such that \( \text{Star}(D) \simeq \text{Star}(k, B) \); let \( T \) be the integral closure of \( D \). Then, \( \ell(T/D) = n(s) \).

If \( \ell(T/D) \leq 2 \), then by [2, Theorem 6.3] or [13, Theorem 3.8] \( \text{Star}(D) \) is a singleton, and thus
\[
\theta(s, q) = \log_q \log_2 1 = \log_q 0 = -\infty.
\]

If \( n(s) = 3 \), then by [8, Theorem 3.1] the cardinality of \( \text{Star}(D) \) does not depend on \( k = D/\mathfrak{m} \). Hence, \( \log_2(\Lambda(s, q)) \) is constant in \( q \), and so \( \theta(s, q) = \log_q \log_2(\Lambda(s, q)) \) goes to 0. \( \square \)

In view of these two cases, we advance the following conjectures.

**Conjecture 1.** For every sequence of pairs of positive integers \( s \), the function \( q \mapsto \theta(s, q) \) has a limit when \( q \to \infty \). Furthermore,

**Conjecture 2.** The limit of \( \theta(s, q) \) as \( q \to \infty \) depends only on \( n(s) \), that is, if \( n(s) = n(t) \), then \( \theta(s, q) \) and \( \theta(t, q) \) have the same limit as \( q \to \infty \).

It is to be noted that Propositions 3.8 and 3.9 are quite flimsy evidence for these conjectures; in particular, Proposition 3.9 would also be true if, instead of the very peculiar function \( q \mapsto \log_q \log_2 \Lambda(s, q) \), we would have taken any function \( q \mapsto \zeta(q) \) with limit 0 as \( q \to \infty \). In the rest of the paper, we will give some justification for this choice by showing that, as \( q \to \infty \), the limit inferior and superior of \( \theta(s, q) \) can be bounded by functions in \( n(s) \) with a polynomial growth (Theorem 5.9) and that Conjecture 2 is true also for \( n = 4 \).
4. The number of subspaces

Let $A \subseteq B$ be a ring extension and let $\mathcal{G} \subseteq \mathcal{F}_B(A)$. Then, a multiplicative operation $\star$ on $(A,B,\mathcal{G})$ is uniquely determined by the set $\mathcal{G}^\star := \{ I \in \mathcal{G} \mid I = I^\star \}$ of its closed ideals. In particular, there is an obvious bound $|\text{Mult}(A,B,\mathcal{G})| \leq 2^{|\mathcal{G}|}$. In this section, we use this fact to bound the number of star operations on $(k,B)$.

Given a finite field $k$ of cardinality $q$, and a $k$-vector space $V$ of dimension $n$, we denote by $Z(q,n)$ the number of vector subspaces of $V$.

**Lemma 4.1.** For every $n$ and every $\epsilon > 0$, there is a $q(n,\epsilon)$ such that

$$Z(q,n) \leq \begin{cases} n \cdot q^{n^2/4+\epsilon(n/2)} & \text{if } n \text{ is even,} \\ n \cdot q^{(n^2-1)/4+\epsilon((n+1)/2)} & \text{if } n \text{ is odd} \end{cases}$$

for all $q \geq q(n,\epsilon)$.

**Proof.** Fix $\epsilon > 0$. Let $Z_t(q,n)$ be the number of $t$-dimensional subspaces of $V$. Then (see e.g. [21, Proposition 1.3.18] or [5, Chapter 13, Proposition 2.1]), $Z_t(q,n)$ is given by the $q$-binomial coefficient

$$\binom{n}{t}_q := \frac{(q^n - 1) \cdots (q^{n-t+1} - 1)}{(q^t - 1) \cdots (q - 1)}.$$

For large $q$, we have

$$q^{n-t+j} - 1 \leq q^{n-t+\epsilon}(q^j - 1)$$

since the dominant term on the right hand side is $q^{n-t+j+\epsilon}$. Hence,

$$\binom{n}{t}_q = \prod_{j=1}^{n-t} \frac{q^{n-t+j} - 1}{q^j - 1} \leq \prod_{j=1}^{t} q^{n-t+\epsilon} = q^{(n-t+\epsilon)}.$$ 

The maximum of the function $t \mapsto t(n - t + \epsilon)$ is in $t_0 := \frac{n+\epsilon}{2}$; checking the integers closer to $t_0$, we obtain that the maximum is in $\frac{n}{2}$ when $n$ is even and in $\frac{n+1}{2}$ when $n$ is odd.

Therefore, if $n$ is even we have

$$Z(q,n) = \sum_{t=0}^{n} Z_t(q,n) \leq \sum_{t=1}^{n} q^{(n/2)(n-(n/2)+\epsilon)} \leq nq^{n^2/4+\epsilon n/2}$$

(where we can forget the zero subspace since the inequalities are not tight). Analogously, if $n$ is odd,

$$Z(q,n) = \sum_{t=0}^{n} Z_t(q,n) \leq \sum_{t=1}^{n} q^{((n+1)/2)(n-((n+1)/2)+\epsilon)} \leq nq^{(n^2-1)/4+\epsilon(n+1)/2}.$$

The claim is proved. \qed
Theorem 4.2. Let $s$ be a sequence of pairs of positive integers and let $n := n(s)$. Then,
\[
\limsup_{q \to \infty} \theta(s, q) \leq \begin{cases} 
\frac{n(n-2)}{4} & \text{if } n \text{ is even,} \\
\frac{(n-1)^2}{4} & \text{if } n \text{ is odd.}
\end{cases}
\]

Proof. By parts (b) and (c) of Proposition 3.3, for large $q$ any star operation on $(k, B_s)$ is a multiplicative operation on $(k, F_1(k, B))$, and thus $|\text{Star}(k, B_s)| \leq 2|F_1(k, B_s)|$, i.e.,
\[
\theta(s, q) \leq \log_q |F_1(k, B_s)|.
\]

The number of $k$-subspaces of $B_s$ containing 1 is the number of $k$-subspaces of a vector space of dimension $n - 1$, i.e., $|F_1(k, B_s)| \leq Z(q, n - 1)$. Hence, for $n$ even,
\[
\limsup_{q \to \infty} \theta(s, q) \leq \limsup_{q \to \infty} \log_q ((n - 1) \cdot q^((n-1)^2 - 1)/4 + \epsilon((n-1+1)/2))
\]
\[
\leq \limsup_{q \to \infty} \left(\frac{(n - 1)^2 - 1}{4} + \frac{\epsilon n}{2}\right)
\]
\[
= \frac{n^2 - 2n}{4} = \frac{n(n - 2)}{4}
\]

using Lemma 4.1 on the odd number $n - 1$ and since $\epsilon > 0$ is arbitrary. The same calculation for $n$ odd gives $\limsup_{q \to \infty} \theta(s, q) \leq \frac{(n-1)^2}{4}$. \hfill $\Box$

The two quadratic functions that bound $\limsup_{q \to \infty} \theta(s, q)$ are rather close to the quadratic functions that give the limit of $\theta((n, 1), q)$ in Proposition 3.8: for example, if $n$ is even, then the difference between the upper bound and the limit of the case $(n, 1)$ is just $\frac{n(n-2)}{4} - \frac{(n-2)^2}{4} = \frac{n-2}{4}$, which is linear instead of quadratic.

5. Lower bounds

Definition 5.1. Let $I \in F_0(k, B)$. The principal star operation generated by $I$ is the largest star operation that closes $I$; we denote it by $*I$. If $A \subseteq F_0(k, B)$, the star operation generated by $A$, denoted by $*_A$, is the largest star operation that closes every element of $G$; equivalently, $*_A = \inf\{*I \mid I \in A\}$.

The definition given above is slightly different from the definition given in [20, Section 4] since we are imposing that $*I$ also closes $k$ (as we want $*I$ to be a star operation and not only a multiplicative operation). However, the two definitions are actually very close.

Proposition 5.2. Let $I, J \in F_1(k, B)$. Then,
\[
J^{*I} = \begin{cases} 
k & \text{if } J = k, \\
\bigcup\{(I : b) \mid bJ \subseteq I\} & \text{otherwise.}
\end{cases}
\]
Proof. Let $v(I)$ be the multiplicative operation generated by $I$ on $(k, B, \mathcal{F}_1(k, B))$, as in [20, Definition 4.2]. Then, $*I$ is just the infimum of $v(k)$ and $v(I)$, and thus

$$J^{*I} = J^{v(k)} \cap J^{v(I)}.$$ 

By the proof of [20, Lemma 4.4], we have $J^{v(I)} = \bigcup\{(I : b) \mid bJ \subseteq I\}$. On the other hand, if $J = k$, then clearly $J^{v(k)} = k$; if $J \neq k$, then $(k : J) = 0$, since if $tJ \subseteq k$, then $t \in k$ (since $1 \in J$) but since $\dim_k J > 1$ the only possibility is $t = 0$. Hence, again by [20, Lemma 4.4],

$$J^{v(k)} = (k : (k : J)) = (k : 0) = B.$$ 

The claim is proved. □

Let $\sim$ be the equivalence relation defined by $I \sim J$ if and only if $*I = *J$. If $G \subseteq \mathcal{F}_0(k, B)$, we denote by $[G]$ the set of equivalence classes containing at least one element of $G$. By definition, $|\text{Star}(k, B)| \geq |[\mathcal{F}_0(k, B)]|$; however, this bound is too weak, since it is not exponential in the cardinality of $[\mathcal{F}_0(k, B)]$, which is typically polynomial in $q$. Hence, we need a stronger criterion.

Lemma 5.3. Let $G \subseteq \mathcal{F}_0(k, B)$ be a subset such that, for every $I \in G$, we have $I^{*G \setminus \{I\}} \neq I$. Then, $|\text{Star}(k, B)| \geq 2^{|G|}$.

Note that the hypothesis implies that no two distinct elements of $G$ are equivalent under $\sim$.

Proof. Let $A \neq B$ two subsets of $G$. Then, without loss of generality there is an $I \in A \setminus B$: we have $I^{*A} \subseteq I^{*I} = I$, so that $I^{*A} = I$, while

$$I^{*I} \supseteq I^{*G \setminus \{I\}} \supseteq I$$

by hypothesis and since $B \subseteq G \setminus \{I\}$. Therefore, $*A \neq *B$. It follows that every subset of $G$ generates a different star operation, and so $|\text{Star}(k, B)| \geq 2^{|G|}$. □

We now want to apply this criterion. We start from the local case.

Proposition 5.4. Let $e, f$ be positive integers and let $n := ef$. Then,

$$\theta((e, f), q) \geq n - 3$$

for every $q$.

Proof. If $n \leq 3$, then $\theta((e, f), q) \geq 0 \geq n - 3$ and we are done. Suppose $n \geq 4$. By definition, $\theta((e, f), q)$ is equal to the number of star operations on $(k, B)$, where $B := L[X]/(X^f)$ for some extension $L$ of $k$ and some $f \geq 1$.

For every $\alpha \in B \setminus k$, consider the submodule $I(\alpha) := (1, \alpha)$. Every such submodule can be obtained in $q^f - q$ ways (through all the $\beta \in I(\alpha) \setminus k$) and thus there are exactly $(q^n - q)/(q^f - q) = (q^{n-1} - 1)/(q - 1)$ different submodules. Let $I$ be the set of the ideals $I(\alpha)$ not containing $X^{f-1}$. 

\section{Asymptotic for the Number of Star Operations}
We want to consider $I(\alpha)^{\ast(\beta)}$. By Proposition 5.2, we have

$$I(\alpha)^{\ast(\beta)} = \bigcap \{ (I(\beta) : \gamma) \mid I(\alpha) \subseteq (I(\beta) : \gamma) \}.$$ 

Suppose $I(\alpha) \subseteq (I(\beta) : \gamma)$: then, if $\gamma$ is a unit of $B$ we have $I(\alpha) \subseteq \gamma^{-1}I(\beta)$, and the two ideals must be equal since they are both 2-dimensional $k$-subspaces of $B$. On the other hand, if $\gamma$ is not a unit, then $\gamma X^{f-1} = 0$ and thus $X^{f-1} \in (I(\beta) : \gamma)$. Therefore, we have two cases:

- if $I(\alpha) \subseteq (I(\beta) : \gamma)$ for some unit $\gamma$, then $I(\alpha)^{\ast(\beta)} = I(\alpha) = \gamma^{-1}I(\beta)$ and $I(\alpha)$ and $I(\beta)$ are in the same class;
- if $I(\alpha) \not\subseteq (I(\beta) : \gamma)$ for all units $\gamma$, then $X^{f-1} \in I(\alpha)^{\ast(\beta)}$.

Note that, if $f = 1$, then $B$ is a field and thus in the second case $I(\alpha) \not\subseteq (I(\beta) : \gamma)$ for all $\gamma \neq 0$, and thus $I(\alpha)^{\ast(\beta)} = B$.

Let $\mathcal{G}$ be a subset of $I$ containing exactly one $I(\alpha)$ for each class with respect to $\sim$. If $I \in \mathcal{G}$, then $X^{f-1} \in I^{\ast\ast}$ for every $J \in \mathcal{G} \setminus \{ I \}$; thus, $X^{f-1} \in I^{\ast\ast(\gamma)}$. Since $X^{f-1} \not\in I$ by definition, by Lemma 5.3 we have $|\text{Star}(k, B)| \geq 2^{[\mathcal{G}]}$.

We now need to estimate $|\mathcal{G}|$. By the reasoning above, the ideals $I(\alpha)$ and $I(\beta)$ can be in the same class only if $I(\beta) = \gamma I(\alpha)$ for some unit $\gamma$. Since $1 \in I(\alpha)$, the ideal $I(\beta)$ can be in this form only if $\gamma^{-1} \in I(\beta)$, and thus there are at most $q^2 - 1$ possibilities; furthermore, $\gamma I(\alpha) = t \gamma I(\alpha)$ for all $t \in k \setminus \{ 0 \}$, and thus the number of such ideals is at most $(q^2 - 1)/(q - 1) = q + 1$. Hence,

$$|\mathcal{G}| \geq \frac{1}{q + 1} \left( \frac{q^{n-1} - 1}{q - 1} - 1 \right) = \frac{q^{n-1} - q}{q^2 - 1} \geq q^{n-3}.$$ 

The claim follows.

The previous proof does not quite work in the non-local case, since in this case $B$ does not have an essential $B$-ideal analogous to $X^{f-1}$. A first attempt is the following.

**Proposition 5.5.** Let $B_1, B_2$ two $k$-algebras. There is an injective, order-preserving map

$$\text{Star}(k, B_1) \times \text{Star}(k, B_2) \hookrightarrow \text{Star}(k, B_1 \times B_2).$$

In particular, $|\text{Star}(k, B_1)| \leq |\text{Star}(k, B_1 \times B_2)|$.

**Proof.** Let $G_1 := F_0(k, B_1)$. For each $I_1 \in \text{Star}(k, B_1)$, let $H_1 := \{ I \in B_2 \mid I \in G_1^{\ast(\gamma)} \}$ and define symmetrically $H_2$. For every pair $(I_1, I_2)$ in the product $\text{Star}(k, B_1) \times \text{Star}(k, B_2)$, let $\iota(I_1, I_2)$ be the star operation generated by $H_1 \cup H_2$; then, $\iota$ is a map from the product to $\text{Star}(k, B_1 \times B_2)$. To show that it is injective, let $J := I \times B_2$ for some $I \in G_1$. Then, for every $L = L_1 \times B_2 \in H_1$, we have

$$(J : L) = (I \times B_2 : L_1 \times B_2) = (I : L_1) \times B_2$$

and thus $J^{\ast\iota} = I^{\ast\iota_1} \times B_2$. On the other hand, if $L = B_1 \times L_2 \in H_2$, then $J^{\ast\iota} = B_1 \times B_2$. Therefore, $J^{\ast(\iota_1, \iota_2)} = I^{\ast(\iota_1, \iota_2)}$; in the same way, if $J = B_1 \times I$, then $J^{\ast(\iota_1, \iota_2)} = B_1 \times I^{\ast\iota_2}$. Hence, $\iota$ is injective and the claim is proved. \qed
The previous proposition works best when $B$ has a local factor $B_i$ such that $n_i = e_i f_i$ is large; in that case, using Proposition 5.4 have $|\text{Star}(k, B)| \geq |\text{Star}(k, B_i)| \geq 2^{q^{n_i - 3}}$, which gives $\theta(s, q) \geq n_i - 3$. However, if every $n_i$ is small with respect to $n$ we need a different kind of estimate.

**Lemma 5.6.** Let $B$ be a finite $k$-algebra, and let $n := \ell_k(B)$. Then, for every $\epsilon > 0$ there is a $q(\epsilon)$ such that if $q \geq q(\epsilon)$ the ring $B_q$ has at least $$(q - 1)^n \geq q^{(1-\epsilon)n}$$ units.

**Proof.** Let $B := B_1 \times \cdots \times B_t$, where $B_i := F_q[x]/(X^{f_i})$ for each $i$. Set $n_i := e_i f_i$. Each $B_i$ has $q^{e_i f_i} = q^{e_i f_i - e_i} = q^{n_i - q^{n_i - e_i}}$ units; thus the number of units of $B$ is at least

$$\prod_{i=1}^t (q^{n_i} - q^{n_i - e_i}) \geq \prod_{i=1}^t q^{n_i - e_i} (q^{e_i} - 1)$$

$$\geq \prod_{i=1}^t q^{n_i - e_i} (q - 1)^{e_i}$$

$$\geq \prod_{i=1}^t (q - 1)^{n_i - e_i} (q - 1)^{e_i} = (q - 1)^n$$

for large $q$. The claim is proved. \qed

**Proposition 5.7.** Let $s := \{(e_1, f_1), \ldots, (e_t, f_t)\}$ be a sequence of pairs of positive integers, and let $n := n(s)$ and $r := e_1 f_1$. If $n - r \geq 3$, then

$$\liminf_{q \to \infty} \theta(s, q) \geq n - r - 2.$$

**Proof.** Since we are only interested in the limit for large $q$, we can suppose that $q > t$, so that we only need to consider subspaces in $F_q(k, B)$.

Let $B_i := F_q[x]/(X^{f_i})$, write $B := B_1 \times \cdots \times B_t$ and $B' := B_1 \times \cdots \times B_{t-1}$, so that $B = B' \times B_t$. By Lemma 5.6, for large $q$ the ring $B'$ has at least $q^{(1-\epsilon)(n-r)}$ units. For every unit $\alpha$ of $B'$ not belonging to $k$, let $I(\alpha) := \langle 1, (\alpha, 0) \rangle$, and let $\mathcal{I}$ be the set of such $I(\alpha)$.

We note that the unique elements of $I(\alpha)$ in the form $(\gamma, 0)$ are those with $\gamma = z\alpha$ for some $z \in k$: hence, the cardinality of $\mathcal{I}$ is equal to

$$\frac{|U(B')|}{q - 1} \geq \frac{q^{(1-\epsilon)(n-r)} - 1}{q - 1} \geq q^{(1-\epsilon)(n-r) - 1}$$

for large $q$. Furthermore, the second component of any element of $I(\alpha)$ belongs to $k$.

By Proposition 5.2, we have

$$I(\alpha)^{\mathcal{I}(\alpha)} \supseteq \bigcap_{\gamma \in \mathcal{I}(\alpha)} (I(\gamma) : \gamma I(\alpha) \subseteq I(\beta)).$$

We claim that if $\gamma \neq 0$ and $\gamma I(\alpha) \subseteq I(\beta)$, then $\gamma$ is a unit of $B$. 

Indeed, let $\gamma := (\gamma_1, \gamma_2)$. Since $\gamma I(\alpha) \subseteq I(\beta)$, we must have $\gamma \cdot 1 \in I(\beta)$ and $\gamma(\alpha, 0) \in I(\beta)$. The second component of $\gamma = \gamma \cdot 1$ is $\gamma_2$, and thus must belong to $k$. If $\gamma_2 = 0$, then $\gamma(\alpha, 0) = (\gamma_1, 0)$ and thus $\gamma_1 = s\beta$ for some $s \in k$; in particular, $I(\alpha) = I(\beta)$.

If $\gamma_2 \neq 0$ and $\gamma_1 = 0$, then $(0, \gamma_2) \in I(\beta)$; however, this would imply that $(1, 0) = (1, 1) - \gamma_2 1 = \gamma \in I(\beta)$, against $\alpha \notin k$.

Suppose $\gamma_1, \gamma_2 \neq 0$. Then, $\gamma_1 = s\beta$ for some $s \in k$; since $\alpha$ is a unit, $s\beta \neq 0$ and thus $s\beta$ is a unit of $B'$, and thus the same must hold for $\gamma_1\alpha$; in particular, $\gamma_1$ must be a unit of $B'$, and thus $\gamma = (\gamma_1, \gamma_2)$ is a unit of $B$, as claimed.

Therefore, if $\gamma \neq 0$ and $\gamma I(\alpha) \subseteq I(\beta)$, then $(I(\beta) : \gamma) = \gamma^{-1}I(\beta)$ has dimension 2, and thus must be equal to $I(\alpha)$. Hence, $I(\alpha)^{\star r(\beta)}$ is either equal to $I(\alpha)$ or to $B$, and in the former case it must be in the form $\gamma^{-1}I(\beta)$ for some unit $\gamma$ of $B$ belonging to $I(\beta)$; in particular, $I(\alpha)$ and $I(\beta)$ must be in the same class. Let $\mathcal{G}$ be a set constructed by taking one representative for each class. There are at most $q^2 - q$ possible units $\gamma$ (for each choice of $\alpha$), and they give $q$ different ideals $\gamma^{-1}I(\beta)$, since $\gamma^{-1}I(\beta) = (s\gamma)^{-1}I(\beta)$ for every $s \in k$. Hence,

$$|\mathcal{G}| \geq \frac{q^{(1-r)(n-r)-1}}{q} = q^{(1-r)(n-r)-2}$$

for large $q$.

As in the proof of Proposition 5.4, $\mathcal{G}$ satisfies the hypothesis of Lemma 5.3, and thus $|\text{Star}(k, B)| \geq 2|\mathcal{G}|$. Using the previous estimate and taking the limit as $q \to \infty$ we have our claim. \hfill $\square$

**Proposition 5.8.** Let $s$ be a sequence of pair of positive integers, and let $n := n(s)$. Then,

$$\liminf_{q \to \infty} \theta(s, q) \geq \begin{cases} \frac{n-4}{2} & \text{if } n \text{ is even}, \\ \frac{n-3}{2} & \text{if } n \text{ is odd}. \end{cases}$$

**Proof.** Let $s := \{(e_1, f_1), \ldots, (e_t, f_t)\}$, and let $n_i := e_i f_i$ for each $i$.

Suppose first that $n$ is even, and let $r$ be the largest of the $n_i$. If $r \leq n/2$, then by Proposition 5.7 we have, for large $q$,

$$\liminf_{q \to \infty} \theta(s, q) \geq n - \frac{n}{2} - 2 = \frac{n}{2} - 2 = \frac{n - 4}{2}.$$ 

On the other hand, if $r > n/2$, then $r \geq (n + 2)/2$, and thus by Propositions 5.4 and 5.5 we have

$$\theta(s, q) \geq r - 3 \geq \frac{n}{2} - 2 = \frac{n - 4}{2},$$

and the claim follows.

Suppose now that $n$ is odd. If $t = 1$ (i.e., if the associated Artinian ring $B$ is local), then by Proposition 5.4 we have $\theta(s, q) \geq n - 3 \geq \frac{n-3}{2}$. If $t > 1$, then there is at least one $n_i$ that is smaller than $n/2$; let it be $r$. Then, $r \leq (n-1)/2$
and, by Proposition 5.7, we have

\[
\liminf_{q \to \infty} \theta(s, q) \geq n - \frac{n - 1}{2} - 2 = \frac{n - 3}{2}.
\]

The claim is proved. □

**Theorem 5.9.** Let \( s \) be a sequence of pair of positive integers, and let \( n := n(s) \). Then,

\[
\begin{cases}
\frac{n - 4}{2} \leq \liminf_{q \to \infty} \theta(s, q) \leq \limsup_{q \to \infty} \theta(s, q) \leq \frac{n(n - 2)}{4} & \text{if } n \text{ is even,} \\
\frac{n - 3}{2} \leq \liminf_{q \to \infty} \theta(s, q) \leq \limsup_{q \to \infty} \theta(s, q) \leq \frac{(n - 1)^2}{4} & \text{if } n \text{ is odd.}
\end{cases}
\]

**Proof.** The first inequality (of both cases) follows from Proposition 5.8, and the last one from Theorem 4.2. □

Note that the limit inferior of the previous theorem is only significant for \( n \geq 5 \). For \( n \leq 3 \) we can apply Proposition 3.9, while we will analyze the case \( n = 4 \) in Section 7.

### 6. Codimension 1

In this section, we consider the subspaces of \( B \) having codimension 1; in particular, we want to show that the number of classes of these ideals (with respect to generating the same star operation) can be bounded above by a function that does not depend on the size of \( k \).

The main tool is the use of canonical ideals. Given an integral domain \( D \) with quotient field \( K \), an ideal \( I \) of \( D \) is a **canonical ideal** of \( D \) if, for every ideal \( J \), we have \( J = (I : K (I : K J)) \); note that there are many equivalent (and more general) definitions (see e.g. [14, Chapter 15]), but we use this one since it is closer to our subject. In particular, we need the following characterization.

**Proposition 6.1.** Let \((D, m)\) be a one-dimensional Noetherian local domain, let \( T \) be its integral closure, and suppose that \((D : T) = m\). Let \( I \in \mathcal{F}_0(D, T) \). Then, \( I \) is a canonical ideal if and only if \( \ell_D(T/I) = 1 \) and \( m \) is the largest ideal of \( T \) contained in \( I \).

**Proof.** By [14, Theorem 15.5], \( I \) is a canonical ideal if and only if \( \ell_D((I : m)/I) = 1 \).

Since \( m \) is a \( T \)-ideal contained in \( I \), we have \( I \subseteq T \subseteq (I : m) \); hence, \( \ell_D((I : m)/I) = 1 \) if and only if \( I : m = T \) and \( \ell_D(T/I) = 1 \). Furthermore, if \( L \) is a \( T \)-ideal contained in \( I \), then \( (I : m) \supseteq (L : m) \), which is greater than \( T \) as soon as \( m \subseteq L \). Hence, \( m \) must be the largest ideal of \( T \) contained in \( I \).

Conversely, if the two conditions hold, we claim that \((I : m) = T\): otherwise, there would be a \( t \in (I : m) \setminus T \), but then \( tm \) would be a \( T \)-ideal contained in \( I \) but not in \( m \), against the hypothesis. Therefore \( \ell_D((I : m)/I) = \ell_D(T/I) = 1 \) is a canonical ideal. □
Suppose now we are in our setting: $k$ is a field and $B$ is a finite $k$-algebra. Following [20], we say that $I \in \mathbf{F}_k(B)$ is a canonical ideal of $(k, B)$ if $*_I$ is the identity; this definition mirrors the definition of $m$-canonical ideals given in [6]. By Proposition 5.2 and the explicit description of the closure generated by identity; this definition mirrors the definition of $m$-canonical ideals given in [6].

**Proposition 6.2.** Let $(D, m)$ be a one-dimensional Noetherian local domain, let $T$ be its integral closure and suppose $(D : T) = m$. Suppose $I$ is a fractional ideal of $D$ satisfying $(D : T) \subseteq I \subseteq T$. Then, $I$ is a canonical ideal of $D$ if and only if its image $\bar{I}$ is a canonical ideal of $(D/m, T/m)$.

**Proof.** By [20, Theorem 6.4 and Corollary 6.5] (see also the discussion after Definition 3.4), there is a bijection between the star operations on $D$ and the star operations on $(D/m, T/m)$; in particular, the star operation generated by $I$ corresponds to the star operation generated by its image $\bar{I}$. The claim follows from the definitions. □

**Corollary 6.3.** Let $B$ be a finite $k$-algebra that is a principal ideal ring, and let $I \in \mathcal{F}_1(k, B)$. Then, $I$ is a canonical ideal of $(k, B, \mathcal{F}_1(A, B))$ if and only if $\ell_k(B/I) = 1$ and $I$ does not contain any nonzero $B$-ideal.

**Proof.** By Proposition 3.5, we can find a principal ideal domain $T$ such that $B$ is a quotient of $T$. Setting $D$ to be the counterimage of $k$, we are in the setting of Proposition 6.2, and then we can apply Proposition 6.1. □

Given a $k$-algebra $B$, let now $\mathcal{H}(B)$ be the set of all $k$-hyperplanes of $B$ containing 1, i.e., the set of $I \in \mathcal{F}_1(k, B)$ such that $\ell_k(B/I) = 1$. We want to estimate in how many different star operations the elements of $\mathcal{H}(B)$ generate, i.e., in how many classes $\mathcal{H}(B)$ is partitioned.

If $I \in \mathcal{F}(A, B)$, we define $Z(I)$ to be the largest $B$-ideal contained in $I$: this is well-defined since if $L_1, L_2 \subseteq I$ are $B$-ideals, then also $L_1 + L_2$ is a $B$-ideal contained in $I$.

**Lemma 6.4.** Let $I, J \in \mathcal{F}(A, B)$, and let $*_I$ be the multiplicative operation generated by $I$. Then, $J + Z(I) \subseteq J^{*_I}$.

**Proof.** Since $J \subseteq J^{*_I}$, we only need to show that $Z(I) \subseteq J^{*_I}$. If $t \in Z(I)$, then $tT \subseteq Z(I) \subseteq I$; in particular, $t(I :_B J) \subseteq I$ and thus $t \in (I :_B (I :_B J)) = J^{*_I}$ (the last equality coming from [20, Lemma 4.4] and Proposition 5.2). □

**Proposition 6.5.** Let $B$ be a finite $k$-algebra that is a principal ideal ring, and let $n := \ell_k(B)$. Then, the following hold.

(a) If $I, J \in \mathcal{H}(B)$, then $*_I = *_J$ if and only if $Z(I) = Z(J)$.

(b) If $\ell_k(B) = n$, then $\mathcal{H}(B)$ is divided into at most $2^n$ classes.

**Proof.** (a) If $Z(I) \neq Z(J)$, then without loss of generality $Z(I) \nsubseteq Z(J)$ and thus $Z(I) \nsubseteq J$. By Lemma 6.4, $B = J + Z(I) \subseteq J^{*_I}$, so that $J \neq J^{*_I}$ and $I$ and $J$ are not in the same class.
Conversely, suppose \( Z(I) = Z(J) \), and consider \( B' := B/Z(I) \). Then, \( I/Z(I) \) and \( J/Z(I) \) are both hyperplanes of \( B' \) not containing any \( B' \)-ideal; by Corollary 6.2, they are canonical ideals of \( B' \). Hence, they generate the identity star operation on \( B' \), and so in \( B \) they generate the map \( *_I : L \mapsto L + Z(I) \).

In particular, \( I \) and \( J \) are in the same class.

(b) Let \( B = B_1 \times \cdots \times B_t \). The ideals of \( B \) are in the form \( I_1 \times \cdots \times I_t \), where each \( I_i \) is either \( B_i \) or an ideal of \( B_i \). Since \( B_i \simeq L_i[X]/(X f_i) \) for some extension \( L_i \) of \( k \), there are \( f_i + 1 \) possible \( I_i \), and thus the number of ideals of \( B \) is \((f_1 + 1) \cdots (f_t + 1)\). However,

\[
\prod_{i=1}^{t} (f_i + 1) \leq \left( \frac{(f_1 + 1) + \cdots + (f_t + 1)}{t} \right)^t \leq \left( \frac{n + t}{t} \right)^t = (1 + \frac{n}{t})^t
\]

using the inequality between geometric and arithmetic mean and the fact that \( f_1 + \cdots + f_t \leq n \). Furthermore, the function \( t \mapsto (1 + \frac{n}{t})^t \) is increasing in \( t \), and thus, since \( t \leq n \), the number of classes is at most \((1 + 1)^n = 2^n\), as claimed.

**Remark 6.6.**

(1) The bound of Proposition 6.5 does not depend on the size of \( k \).

(2) Not all ideals of \( B \) are equal to \( Z(I) \) for some ideal \( I \) of codimension 1: for example, \( B \) itself doesn’t. Another case are the subspaces that are themselves hyperplanes: in that case, we should have \( I = Z(I) \), which is impossible if \( 1 \in I \).

(3) If \( n = 3 \), then the bound of Proposition 6.5 gives \(|\text{Star}(k, B)| \leq 65\) for all choices of \( B \). By considering in more detail the different cases, and excluding the impossible \( B \)-ideals, it is possible to obtain much tighter bounds; for example, if \( B = k^3 \), then we have only three possible \( Z(I) \neq (0) \) (the ones in the form \( I_1 \times I_2 \times I_3 \) with one \( I_i \) equal to \( k \) and two \( I_j \) equal to 0), and thus \(|\text{Mult}_0(k, B)| \leq 1 + 2^3 = 9\), which is the exact value of \(|\text{Star}(k, B)| \) by [8, Theorem 3.1(2)] and Proposition 3.9.

## 7. The case \( n = 4 \)

In this section, we are going to prove Conjecture 2 for \( n(s) = 4 \). In this case, Theorem 5.9 gives

\[
0 \leq \lim \inf_{q \to \infty} \theta(s, q) \leq \lim \sup_{q \to \infty} \theta(s, q) \leq 2,
\]

while Proposition 3.8 says that the limit of \( \theta((n, 1), q) \) is 1. Hence, we need to prove that \( \theta(s, q) \to 1 \) for every \( s \).

We start from the upper bound.
Lemma 7.1. Let $k$ be a finite field of cardinality $q$, let $s := \{(e_1, f_1), \ldots, (e_t, f_t)\}$ be a sequence of pairs of positive integers and let $B$ be the Artinian ring associated to $s$. Let $e := \sum_i e_i$ and $n := \ell_k(B) = \sum_i e_i f_i$. Let $\Sigma := \{\alpha \in B \mid \alpha^2 + ra + s = 0 \text{ for some } r, s \in k\}$. Then,

$$|\Sigma| \leq q^{n-e+1} + 2^t(q^2 - q).$$

Proof. Let $B = B_1 \times \cdots \times B_t$, where each $B_i$ is a local $k$-algebra, and let $n_i := \ell_k(B_i)$. Let $\pi_i : B_i \to L_i$ be the quotient of $B_i$ on its residue field $L_i$.

Let $r, s \in k$, and consider the equation $f(X) = X^2 + rX + s$. Let $S_i(f)$ be the set of solutions of $f(X) = 0$ in $B_i$, and suppose that $S_i \neq \emptyset$. If $\alpha \in S_i$, then we can factorize $f(X)$ as $(X - \alpha)(X - \beta)$ for some $\beta \in B_i$. We distinguish two cases.

If $f(X)$ has simple roots in the algebraic closure $\overline{k}$ of $k$, then the images of $\alpha$ and $\beta$ in the residue field of $B_i$ are distinct. Hence, for every $\gamma \in S_i$ one of $\pi_i(\gamma - \alpha)$ and $\pi_i(\gamma - \beta)$ is a unit, and thus $(\gamma - \alpha)(\gamma - \beta) = 0$ implies that $\gamma = \alpha$ or $\gamma = \beta$. Thus, $|S_i(f)| \leq 2$.

If $f(X)$ has a double root over $\overline{k}$, then all roots of $f(X)$ in $B_i$ must belong to $\pi_i^{-1}(\overline{\kappa})$; since the latter is a coset of an ideal of $B_i$, we have $|S_i(f)| \leq q^{n_i - e_i}$. Let now $S(f)$ be the set of solutions of $f(X) = 0$ in $B$. Then, $S(f) = S_1(f) \times \cdots \times S_t(f)$; thus, if $f(X)$ has simple roots in $\overline{k}$, then $|S(f)| \leq 2^t$, while if $f(X)$ has a double root, then $|S(f)| \leq \prod_i q^{n_i - e_i} = q^{n-e}$.

There are exactly $q$ polynomials of degree 2 with a double root (since $k$ is finite, hence perfect), and thus $q^2 - q$ polynomials with single roots. Hence,

$$|\Sigma| \leq (q^2 - q) \cdot 2^t + q \cdot q^{n-e} = q^{n-e+1} + 2^t(q^2 - q) \leq q^{n-t+1} + 2^t(q^2 - q),$$

as claimed. \qed

Proposition 7.2. Suppose $n(s) = 4$. Then,

$$\limsup_{q \to \infty} \theta(s, q) \leq 1.$$

Proof. Let $B$ be the ring associated to $s$, and let $G := F_1(k, B)$. Let $G_i := \{I \in G \mid \dim_k I = i\}$, and let $[G_i]$ denote the set of equivalence classes of $G_i$ with respect to the relation of generating the same star operation. Then, $G_0$ is empty, while $G_1$ and $G_3$ are both singletons: the former is $\{k\}$, the latter is $\{B\}$. Both are contained in $G^*$ for every star operation $\star$ on $(k, B)$, and thus $|\text{Star}(k, B)| \leq 2|[G_2]| + |[G_3]|$.


Consider now $G_2$. Then,

$$|G_2| = Z_1(q, 3) = \binom{3}{1} = \frac{q^2 - 1}{q - 1} = q^2 + q + 1.$$
Let $\mathcal{I}$ be the set of the subspaces in the form $\langle 1, \alpha \rangle$, where $\alpha$ is a unit of $B$ not belonging to $k$; clearly, $\mathcal{I} \subseteq \mathcal{G}_2$. By Lemma 5.6, $B$ has at least $(q - 1)^4$ units; furthermore, every $I(\alpha)$ contains at most $q^2 - q$ of them (not counting those in $k$). Thus,

$$|\mathcal{I}| \geq \frac{(q - 1)^4 - q}{q^2 - q} = \frac{(q - 1)^3 - 1}{q} = q^2 - 3q + 3 - \frac{2}{q} \geq q^2 - 3q + 3.$$

In particular, $|\mathcal{G}_2 \setminus \mathcal{I}| \leq q^2 + q + 1 - (q^2 - 3q + 3) = 4q - 2$.

Let $\alpha$ be a unit. Then, $\alpha^{-1}I(\alpha) = \alpha^{-1}(1, \alpha) = (1, \alpha^{-1}) = I(\alpha^{-1})$. We have that $I(\alpha) = I(\alpha^{-1})$ if and only if $\alpha^{-1} \in \langle 1, \alpha \rangle$, that is, if and only if $\alpha$ satisfies an equation of degree 2 with coefficients in $k$. Since every element of $I(\alpha)$ is in the form $s + ta$ for some $s, t \in k$, we have that $\alpha^{-1}I(\alpha) = I(\alpha)$ if and only if $\beta^{-1}I(\alpha) = I(\alpha)$ for some unit $\beta \in I(\alpha)$. Therefore, $\mathcal{I}$ can be partitioned into two classes:

- $\mathcal{I}_0 := \{ I(\alpha) \mid \alpha^{-1}I(\alpha) = I(\alpha) \}$;
- $\mathcal{I}_1 := \{ I(\alpha) \mid \alpha^{-1}I(\alpha) \neq I(\alpha) \}$.

Each element of $\mathcal{I}_1$ contains at least $q^2 - 2q$ units not in $k$ ($q^2$ elements, minus $q$ in $k$, minus at most $q$ that are not units). Thus, for each subspace there are at least $(q^2 - 2q)/(q - 1) = q - 1 + \frac{1}{q - 1} \geq q - 2$ equivalent subspaces, and thus (applying again Lemma 7.1) the number of classes is at most

$$|\{\mathcal{I}_1\}| \leq \frac{q^2 + q + 1 - (q + 16)}{q - 2} \leq q + 4.$$

Each subspace in $\mathcal{I}_0$ is equivalent only to itself; to estimate its cardinality, we distinguish two cases.

If $t \geq 2$, by Lemma 7.1 there are at most $q^{n-t+1} + 2^t(q^2 - q)$ elements that are solutions of an equation of degree 2; hence, they can fill at most

$$\frac{q^{n-t+1} + 2^t(q^2 - q)}{q^2 - 2q} = \frac{q^{n-t} + 2^t(q - 1)}{q - 1} \geq q^{n-t-1} + 2^t \geq q + 16
$$

ideals, i.e., $|\mathcal{I}_0| \leq q + 16$. Therefore,

$$|\text{Star}(k, B)| \leq 2|\mathcal{G}_2| + |\mathcal{G}_2 \setminus \mathcal{I}| + |\mathcal{I}_0| + |\mathcal{I}_1| \leq 2^4 + 4q + 2 + q + 16(q + 4) = 2^{6q + 26}
$$

and

$$\limsup_{q \to \infty} \theta(s, q) \leq \limsup_{q \to \infty} \log_q \log_2(2^{6q + 26}) = \limsup_{q \to \infty} \log_q(6q + 26) = 1,$$

as claimed.

Suppose $t = 1$. Then, $s = (e, f)$ with $ef = 4$, and thus we have four possibilities: $(4, 1)$, $(2, 2)$, $(1, 4)$. The first one is exactly the one considered in Proposition 3.8, and thus the claim holds. The last one corresponds to the star operations on the ring $A := k[[X^4, X^5, X^6, X^7]]$, for which $|\text{Star}(A)| = 2^{2q + 1} + 2^{q + 1} + 2$ (see [22]), and thus the limit of $\theta(s, q)$ is again 1.

The case $s = (2, 2)$ correspond to $B = L[X]/(X^2)$, where $L$ is the field of cardinality $q^2$. By Lemma 7.1, we have that the number of solutions to
equations of degree 2 is at most $q^{1-2+1} + 2(q^2 - q) = q^3 + 2(q^2 - q)$. Reasoning as above, we get $|\mathcal{L}_0| \leq q + 5$, and so

$$|\text{Star}(k, B)| \leq 2^{q^4+q^2+q+q+q} = 2^{q^6+15}.$$ 

Hence, $\limsup_q \theta(s, q) \leq 1$, as claimed. \hfill \Box

To study the limit inferior, we need to reason by cases. Let $s = \{(e_1, f_1), \ldots, (e_t, f_t)\}$, and let $\{n_1, \ldots, n_t\}$ be a partition of $n := n(s)$. In particular, if $n = 4$, then we have five possible partitions:

- $4$
- $3 + 1$
- $2 + 1 + 1$
- $1 + 1 + 1 + 1$
- $2 + 2$

Note that each of the previous partition may correspond to more than one ring $B$. For example, the case $3 + 1$ is further subdivided into the cases $s = \{(3, 1), (1, 1)\}$ (corresponding to $B = L \times k$, where $L$ is an extension of $k$ of degree 3) and $s = \{(1, 3), (1, 1)\}$ (corresponding to $B = k[X]/(X^3) \times k$).

**Proposition 7.3.** Preserve the notation above. If $n_1 = 4$, then $\liminf_q \theta(s, q) \geq 1$.

**Proof.** Apply Proposition 5.4: $s = \{(e, f)\}$ and thus $\theta((e, f), q) \geq 4 - 3 = 1$. \hfill \Box

**Proposition 7.4.** Preserve the notation above. If $e_i = f_i = 1$ for some $i$, then $\liminf_q \theta(s, q) \geq 1$.

**Proof.** We can apply Proposition 5.7 with $r = 1$, obtaining $\liminf_q \theta(s, q) \geq 4 - 1 - 2 = 1$. \hfill \Box

The only case remaining is the partition $2 + 2$. To examine it, we apply a variant of the proof of Proposition 5.4.

**Proposition 7.5.** Suppose $s = \{(e_1, f_1), (e_2, f_2)\}$ with $e_1 f_1 = e_2 f_2 = 2$. Then, \n
$$\liminf_{q \to \infty} \theta(s, q) \geq 1.$$ 

**Proof.** Let $B = B_1 \times B_2$ be the ring associated to $s$.

Suppose first that $B_1 = L$ is the extension of degree 2 of $k$. Then, $B_1$ has $q^2 - q$ units not belonging to $k$, while $B_2$ has at least $q^2 - 2q$ of them: hence, $B$ has at least $q^2(q-1)(q-2)$ of these unit. For every such unit $\alpha$ of $B$, let $I(\alpha) := \{1, \alpha\}$, and let $\mathcal{I}$ be the set of all $I(\alpha)$. No element of $I(\alpha)$ (different from 0) has a component equal to 0: otherwise, setting $\alpha = (\alpha_1, \alpha_2)$, we would have $s + r\alpha_i = 0$ for some $s, r \in k$ not both 0, against the fact that $\alpha_i$ is not in $k$. Therefore, each there are $q^2 - q$ elements $\beta$ such that $I(\alpha) = I(\beta)$, and so $\mathcal{I}$ has at least $\frac{q^2(q-1)(q-2)}{q^2-q} = q(q-2)$ elements.

Let $\gamma = (\gamma_1, \gamma_2) \in I(\alpha)$: we claim that $J := (I(\alpha) : \gamma)$ cannot have dimension 3 over $k$. 

If $\gamma = 0$, then $(0, \gamma_2, \alpha_2) \in I(\alpha)$; then we must have $\gamma_2 = 0$ and since $\alpha_2$ is a unit, this implies that $\gamma_2 = 0$, i.e., that $\gamma = 0$ and thus $J = B$. If $\gamma \neq 0$, then $\gamma_1$ is a unit of $L$. If $\dim_k J > 2$, then, $J \cap (B_1 \times \{0\})$ must be nontrivial, i.e., there would be some $\beta := (\beta_1, 0) \neq 0$ such that $\beta \in J$. However, $\beta \gamma = (\beta_1, 0)(\gamma_1, \gamma_2) = (\beta_1 \gamma_1, 0) \neq (0, 0)$ since $\gamma_1$ is a unit and $\beta_1 \neq 0$. Hence, if $\gamma \neq 0$, then $\dim_k J = 2$, while if $\gamma = 0$, then $J = B$ and $\dim_k J = 4$.

Hence, $I(\alpha)^{s(\theta)}$ is equal either to $I(\alpha)$ (if $\gamma^{-1} I(\alpha) = I(\beta)$ for some unit $\gamma \in I(\alpha)$) or to $B$; in the former case $I(\alpha)$ and $I(\beta)$ are in the same class, in the latter they belong to different classes. As in the proof of Proposition 5.4, we have $q^2 - 1$ units $\gamma$ in $I(\alpha)$, and if $t \in k \setminus \{0\}$, then $(t \gamma)^{-1} I(\alpha) = \gamma^{-1} I(\alpha)$, and thus each class contains at most $(q^2 - 1)/(q - 1) = q + 1$ ideals of this kind.

Let $G$ be a set of representatives of the classes of $I$: then,

$$|G| \geq \left\lceil \frac{|I|}{q + 1} \right\rceil \geq \frac{q(q - 2)}{q + 1} \geq q - 3.$$

By Lemma 5.3, it follows that $|\text{Star}(k, B)| \geq 2^{q-3}$, and thus $\lim \inf_q \theta(s, q) \geq \lim \inf_q \log_q (q - 3) = 1$, as claimed.

Clearly, if $B_2 = L$, then the argument is identical. Suppose thus that $B_1 \neq L \neq B_2$: then, $B_1$ and $B_2$ must be isomorphic to $k[X]/(X^2)$. Each $B_i$ has $q^2 - 2q$ units not belonging to $k$: we choose those units $\alpha = (\alpha_1, \alpha_2)$ such that the image of $\alpha_1$ and $\alpha_2$ in $k$ are distinct. Thus, we obtain $(q^2 - 2q)(q^2 - 3q) = q^2(q - 2)(q - 3)$ possible $\alpha$. The rest of the reasoning proceeds in the same way, obtaining a bound $|G| \geq q - c$ for some constant $c$, from which the claim follows.

**Theorem 7.6.** Let $s$ be a sequence of pairs of positive integers with $n := n(s) = 4$. Then,

$$\lim_{q \to \infty} \theta(s, q) = 1.$$

**Proof.** By Proposition 7.2, $\lim \sup_q \theta(s, q) \leq 1$. By Propositions 7.3, 7.4 and 7.5 (and the discussion before Proposition 7.3), on the other hand, $\lim \inf_q \theta(s, q) \geq 1$. Hence, the limit exists and is equal to 1.

The previous theorem does not allow by itself an explicit determination of the number of star operations on $(k, B)$, mainly because for every $s$ it is necessary to consider a different number of special cases, which give a different counting. (However, if one follows the proofs in a special case it is possible to obtain some more explicit estimates.) In two cases, the cardinality of $\text{Star}(k, B)$ has been determined explicitly:

- if $s = \{(4, 1)\}$, then $B = F$ (where $F$ is the extension of $k$ of degree 4) and the star operations on $(k, B)$ correspond to the star operations on the pseudo-valuation domain $A := k + XF[[X]]$; in this case,

$$|\text{Star}(A)| = 2^{q+1} + 1$$

by the results in [15] and [18];
if \( s = \{(1,4)\} \), then \( B = k[X]/(X^4) \), or in domain terms we are in the residually rational case \( A := k[[X^4,X^5,X^6,X^7]] \); in this case,

\[
\|\text{Star}(A)\| = 2^{2q+1} + 2^{q+1} + 2
\]

by [22].

We now show how to obtain a precise counting in a further special case, namely when \( B = L \times k \) and \( L \) is the extension of \( k \) of degree 3.

**Example 7.7.** Let \( B := L \times k \), and let \( \mathcal{G}_2 \) and \( \mathcal{G}_3 \) be, respectively, the set of \( k \)-subspaces of \( B \) having dimension 2 and 3 over \( k \) that contain 1.

Let \( \mathcal{G} := \mathcal{F}_3(k,B) = \mathcal{F}_1(k,B) \) (in this case \( t = 2 \) and thus the two sets are equal). On the set \( [\mathcal{G}] \) of classes, define \( [I] \leq [J] \) if and only if \( *_{I} \geq *_{J} \). Then, \( \leq \) is a partial order on \( \mathcal{G} \), and the set \( [\mathcal{G}^{*}] := \{[I] \mid *_{I} = I\} \) is a downset for every \( * \in \text{Star}(k,B) \). See [20, Definition 4.7 onwards] for more information about this order.

As in the proof of Proposition 7.2, let \( \mathcal{G}_{i} \) be the set of \( I \in \mathcal{F}_1(k,B) \) having dimension \( i \) over \( k \).

By Proposition 6.5(a), the class of \( I \in \mathcal{G}_3 \) depends only on the largest \( B \)-ideal \( Z(I) \) contained into \( I \). There are four ideals of \( B \): the zero ideal, \( \{0\} \times B_2 \), \( B_1 \times \{0\} \) and \( B_1 \times B_2 \). In particular, the latter two cannot be in the form \( Z(I) \), since \( B = B_1 \times B_2 \) has dimension 4, while \( B_1 \times \{0\} \) has dimension 3 and does not contain 1. Hence, we have two classes:

- \( \mathcal{G}_{3,\text{can}} := \{I \mid Z(I) = \{(0,0)\}\} \): these are the canonical ideals;
- \( \mathcal{G}_{3,1} := \{I \mid Z(I) = \{0\} \times B_2\} \).

In particular, the elements of \( \mathcal{G}_{3,\text{can}} \) close every \( k \)-subspace, and thus \( \mathcal{G}_{3,\text{can}} \) is the maximum of \( ([\mathcal{G}], \leq) \). On the other hand, the elements of \( \mathcal{G}_{3,1} \) close exactly the subspaces \( J \) such that \( \{(0) \times B_2\} J \subseteq J \), and the only subspace satisfying this condition is \( R(1) := \langle (1,1),(1,0) \rangle = k \times k \). Note that \( R(1) \) does not close any other subspace different from \( k \), because there is no other subspace containing \( \{0\} \times B_2 \). Thus, we have the following partial graph of \( [\mathcal{G}] \):

\[
\mathcal{G}_{3,\text{can}} \rightarrow \mathcal{G}_{3,1} \rightarrow [R(1)] \rightarrow [k].
\]

Consider now \( I \in \mathcal{G}_2 \). Then, we can write \( I = \langle (1,1),(\alpha,\beta) \rangle \) for some \( (\alpha,\beta) \in B \). Since \( \beta \in k \), we can suppose without loss of generality that \( \beta = 0 \), i.e., that \( I = R(\alpha) := \langle (1,1),(\alpha,0) \rangle \). If \( \alpha \in k \), then we have \( R(\alpha) = R(1) \) (see above) and thus it is enough to consider the case \( \alpha \notin k \).

There are \( q^2 - q \) of such \( \alpha \), and each subspace can be generated by \( q - 1 \) of them; hence, we obtain \( q^2 + q \) ideals in this form. By the proof of Proposition 5.7, every equivalence class of them contains \( q \) subspaces, and they are not comparable under \( \leq \). Furthermore, by direct calculation \( (I(\alpha) : (\alpha,0)) = R(1) \) (so \( |R(1)| \leq |I(\alpha)| \) for every \( \alpha \), while no element of \( \mathcal{G}_{3,1} \) is closed by \( I(\alpha) \).
Thus, we obtain the following complete picture of $[G]$:

$$
\begin{align*}
G_{3,1} & \rightarrow [R(1)] \rightarrow [A] \\
G_{3,\text{can}} & \rightarrow [R(\alpha_1)] \\
\vdots & \\
[& R(\alpha_{q+1})]
\end{align*}
$$

Hence, there are $2^{q+2} + 2$ nonempty downsets:

- the whole $[G]$;
- $2^{q+2} - 1$ downsets in the form $X \cup \{[A], R[1]\}$, for nonempty $X \subseteq \{G_{3,1}, R(\alpha_1), \ldots, R(\alpha_{q+1})\}$;
- $[A]$ and $[A] \cup [R(1)]$.

By direct inspection and by [20, Proposition 4.10], all these downset give rise to a star operation, and thus $|\text{Star}(k, B)| = 2^{q+2} + 2$ star operations.

We note that, in the three cases considered explicitly for $n = 4$, the number of star operations is a polynomial $f(X)$ evaluated in $X = 2^q$: indeed, for $s = \{(4,1)\}$ the polynomial is $f(X) = 2X + 1$, for $s = \{(1,4)\}$ we have $f(X) = 2X^2 + 2X + 2$, and for $s = \{(3,1), (1,1)\}$ we have $f(X) = 4X + 2$. This fact leads to the following final conjecture.

**Conjecture 3.** For every $s$ such that $n(s) = 4$ there is a polynomial $f(X) \in \mathbb{Z}[X]$ such that $\Lambda(s, q) = f(2^q)$ for every $q$.

This conjecture cannot be generalized to higher lengths: for example, in the case $s = \{(5,1)\}$, the number of star operations is equal to $(q^2 + 5)2^{q^2} - (q^2 - 1)$ [18, Theorem 4.3].

**References**


Dario Spirito
Dipartimento di Matematica e Fisica
Università degli Studi “Roma Tre”
Roma, Italy
AND
Dipartimento di Matematica
Università di Padova
Padova, Italy

Email address: spirito@mat.uniroma3.it; spirito@math.unipd.it