Finite Fields and Their Applications 56 (2019) 17–30

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Vector subspaces of finite fields and star operations on pseudo-valuation domains

Dario Spirito

Dipartimento di Matematica e Fisica, Università degli Studi "Roma Tre", Roma, Italy

ARTICLE INFO

Article history:
Received 16 January 2018
Received in revised form 25 September 2018
Accepted 3 November 2018
Available online xxxx
Communicated by L. Storme

MSC:
05A10
11B65
13A15
13A18
13G05

Keywords:
q-binomial coefficients
Star operations
Pseudo-valuation domains

ABSTRACT

Given an extension of finite fields $F \subseteq L$, we study the number of the equivalence classes of F-vector subspaces of L modulo multiplication by elements of L, obtaining an exact formula and some bounds. We then apply the results obtained to the study of the set of F-star operations on L, which correspond to star operations on a pseudo-valuation domain R.

1. Introduction

Let $F := \mathbb{F}_q$ be a finite field, and let V be an n-dimensional vector space over F. It is well-known (see e.g. [7, Proposition 1.3.18] or [4, Chapter 13, Proposition 2.1]) that the

E-mail address: spirito@mat.uniroma3.it.

https://doi.org/10.1016/j.ffa.2018.11.001
1071-5797/

number of vector subspaces of V of dimension t is given by the *q-binomial coefficient* (or *Gaussian binomial coefficient*) $\binom{n}{t}_q$, defined as

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

Suppose now V is equal to $L := \mathbb{F}_{q^n}$, the extension of F of degree n. Then, the multiplicative group of L acts on the set of the F-subspaces of L; the purpose of this paper is to study the number of orbits of this action, in particular when we also fix the dimension of the subspaces. We obtain an explicit formula for the number of orbits composed by t-dimensional subspaces (Theorem 2.1) and some bounds both for the number of orbits with fixed dimension and for the overall number of orbits (Propositions 2.5 and 2.6).

In Section 3, we introduce F-star operations on L, based on the definition of star operations on an integral domain; we then formalize the link between the two concepts (implicitly present in [6]) by finding an order-preserving bijection between the set of F-star operations on L and the set of star operations on a pseudo-valuation domain (Theorem 3.1). We then use the results on t-dimensional subspaces to estimate the growth of the number of star operations as $q \to \infty$ or as $n \to \infty$ (Theorem 3.7). In Section 4, we calculate explicitly this number when $n \leq 5$.

2. Vector subspaces

Let $F := \mathbb{F}_q$ be the field with q elements (q a prime power), and let $L := \mathbb{F}_{q^n}$ be its extension of degree n. We denote by $\mathcal{O}(L,F)$ the set of F-vector subspaces of L, and by $\mathcal{O}_t(L,F)$ the set of subspaces having dimension t.

The multiplicative group L^* of L acts on $\mathcal{O}(L,F)$ by multiplication; furthermore, this action restricts to every $\mathcal{O}_t(L,F)$ [6, Proposition 2.4]. We denote by $\ell(q,n,t)$ the number of orbits of $\mathcal{O}_t(L,F)$ under this action. Equivalently, $\ell(q,n,t)$ is the number of equivalence classes of $\mathcal{O}_t(L,F)$ under the equivalence relation $\sim$ such that $V \sim W$ if $V = \beta W$ for some $\beta \in L$.[1]

Our first result is an explicit formula for $\ell(q,n,t)$. We use μ to denote the Möbius function, and (a,b) to denote the greatest common divisor of a and b.

Theorem 2.1. *Let q be a prime power, and $n > t > 0$ be integers. Then,*

$$\ell(q,n,t) = \frac{q-1}{q^n-1}\binom{n}{t}_q + \frac{1}{q^n-1}\sum_{\substack{d|(t,n)\\ d\neq 1}}\left(\sum_{e|d}\mu\left(\frac{d}{e}\right)q^e\right)\binom{n/d}{t/d}_{q^d}$$

[1] The number $\ell(q,n,t)$, defined in the latter way, was denoted by l_t in [6]; we changed the notation to make explicit the dependence on q and n.

$$= \frac{1}{q^n-1}\left[\sum_{d|(t,n)}\left(\sum_{e|d}\mu\left(\frac{d}{e}\right)q^e\right)\binom{n/d}{t/d}_{q^d}\right] - \frac{1}{q^n-1}\binom{n}{t}_q.$$

Proof. By Burnside's lemma,

$$\ell(q,n,t) = \frac{1}{|L^*|}\sum_{\alpha\in L^*}|\mathcal{O}_t(L,F)^\alpha|,$$

where $\mathcal{O}_t(L,F)^\alpha$ is the set of subspaces that are fixed by α. However, a t-dimensional subspace W belongs to $\mathcal{O}_t(L,F)^\alpha$ if and only if it is an $F(\alpha)$-vector space; hence, $\mathcal{O}_t(L,F)^\alpha$ is exactly the set of $F(\alpha)$-vector subspaces of L having dimension t/d, where $d := [F(\alpha):F]$. Thus,

$$\ell(q,n,t) = \frac{1}{|L^*|}\sum_{\alpha\in L^*}|\mathcal{O}_{t/[F(\alpha):F]}(L,F(\alpha))|. \tag{1}$$

Let now $\theta(d)$ be the number of elements $\alpha\in L$ such that $[F(\alpha):F]=d$. Then, $q^n=\sum_{d|n}\theta(d)$, and thus by the Möbius inversion formula we have

$$\theta(d) = \sum_{e|d}\mu\left(\frac{d}{e}\right)q^e. \tag{2}$$

Let now F_d be the subfield of L having degree d over F. Then, (1) can be rewritten as

$$\ell(q,n,t) = \frac{1}{|L^*|}\sum_{d|(t,n)}\sum_{\substack{\alpha\in L^*\\ F_d=F(\alpha)}}|\mathcal{O}_{t/d}(L,F_d)|.$$

For any d, the number of times $|\mathcal{O}_{t/d}(L,F_d)|$ appears in this equality is $q-1=\theta(1)-1$ if $d=1$, while it is equal to $\theta(d)$ if $d>1$; hence,

$$\ell(q,n,t) = \frac{q-1}{q^n-1}|\mathcal{O}_t(L,F)| + \frac{1}{q^n-1}\sum_{\substack{d|(t,n)\\ d\neq 1}}\theta(d)|\mathcal{O}_{t/d}(L,F_d)|.$$

Substituting $\theta(d)$ with (2) and $|\mathcal{O}_{t/d}(L,F_d)|$ with $\binom{n/d}{t/d}_{q^d}$ we have the first formula. To prove the second, it is enough to note that, if $d=1$, then

$$\sum_{e|d}\mu\left(\frac{d}{e}\right)q^e\binom{n/d}{q/d}_{q^d} = q\binom{n}{t}_q.$$

The claim follows. □

Corollary 2.2. *Let q be a prime power, and $n > t > 0$ be integers. Then, the following hold.*

(a) $\ell(q,n,t) = \ell(q,n,n-t)$.

(b) *If t and n are coprime, then* $\ell(q,n,t) = \dfrac{q-1}{q^n-1}\binom{n}{t}_q$.

(c) $\ell(q,n,1) = \ell(q,n,n-1) = 1$.

Proof. We have always $(t,n) = (t,n-t)$; furthermore, for every $d|(t,n)$, we have $\frac{n-t}{d} = \frac{n}{d} - \frac{t}{d}$, and thus $\binom{n/d}{t/d}_{q^d} = \binom{n/d}{(n-t)/d}_{q^d}$. It follows that the expression for $\ell(q,n,t)$ given by Theorem 2.1 does not change passing from t to $n-t$. This proves (a). (b) follows easily from Theorem 2.1, while (c) from parts (a) and (b). □

Part (c) of the previous corollary can be seen as a generalization of [6, Lemma 2.12].

While the q-binomial coefficients have a "pyramidal" behavior, i.e., $\binom{n}{t}_q$ increases as t goes from 1 to $\lfloor \frac{n}{2} \rfloor$ and decreases as t goes from $\lceil \frac{n}{2} \rceil$ to n, the same does not happen for the numbers $\ell(q,n,t)$; the reason is that t may have many factors in common with n while $t+1$ does not. For example, $\ell(2,24,6) > \ell(2,24,7)$.

Proposition 2.3. *Fix two integers $n > t$. There is a monic polynomial $\phi_{n,t} \in \mathbb{Z}[X]$ of degree $(t-1)(n-t-1)$ such that $\phi_{n,t}(q) = \ell(q,n,t)$ for every prime power q.*

Proof. Clearly, $\phi := \phi_{n,t}$ is a rational function. Moreover, $\phi(q)$ is an integer for every prime power q; by [2, Proposition X.1.1], ϕ is a polynomial with rational coefficients, and hence $\phi = h/n$ for some $h \in \mathbb{Z}[X]$ and an integer n such that $(h,n) = 1$ in $\mathbb{Z}[X]$.

Also, reducing to the same denominator, we can write ϕ as a quotient f/g, where $f, g \in \mathbb{Z}[X]$ and g is the product of binomials of the form $X^a - 1$. Therefore, n must divide g. However, g has no constant factors (except 1); hence, n must be 1 and $\phi \in \mathbb{Z}[X]$.

To calculate the degree of ϕ, we calculate the degree of each of its summands. Firstly, we note that

$$\binom{a}{b}_p = \frac{(p^a-1)(p^{a-1}-1)\cdots(p^{a-b+1}-1)}{(p^b-1)(p^{b-1}-1)\cdots(p-1)} = \prod_{i=0}^{b-1} \frac{p^{a-i}-1}{p^{b-i}-1},$$

and thus

$$\deg \binom{n/d}{t/d}_{q^d} = \frac{t}{d} d \left(\frac{n}{d} - \frac{t}{d} \right) = \frac{t(n-t)}{d}.$$

Hence,

$$\deg \left[\frac{1}{q^n-1} \left(\sum_{e|d} \mu\left(\frac{d}{e}\right) q^e \right) \binom{n/d}{t/d}_{q^d} \right] = d + \frac{t(n-t)}{d} - n = \frac{(t-d)(n-t-d)}{d}.$$

As a function of d, the right hand side is strictly decreasing for $0 < d \leq t(n-t)$; since $d|(n,t)$, this inequality is always satisfied. In particular, the maximum is reached for $d = 1$, where its value is $(t-1)(n-t-1)$, and so the degree of ϕ is $(t-1)(n-t-1)$. Furthermore, its leading term comes from the summand $\frac{q-1}{q^n-1}\binom{n}{t}_q$, and thus must be 1. Hence, ϕ is monic. □

In particular, if we fix n and t, the previous proposition implies that the order of growth of $\ell(q,n,t)$ is $q^{(t-1)(n-t-1)}$; using the big-O notation, this means that, when n and t are fixed,

$$\ell(q,n,t) = q^{(t-1)(n-t-1)} + O(q^{(t-1)(n-t-1)-1})$$

as $q \to \infty$. We can also prove a slightly more precise bound; we first state a lemma.

Lemma 2.4. *Let q, d be positive integers, with $d > 1$. Then,*

$$0 < \sum_{e|d} \mu\left(\frac{d}{e}\right) q^e \leq q^d - 1.$$

Proof. Let $\psi(d,q)$ be the sum. Then, ψ is a polynomial in q of degree d where each coefficient is $+1$ or -1; furthermore, the leading coefficient is 1 (since it is equal to $\mu(1)$) and the coefficient corresponding to the second largest monomial is -1 (since it is equal to $\mu(p)$, where p is the minimal prime dividing d). The claim follows. □

Proposition 2.5. *Let q be a prime power and $n > t$ be positive integers. Then, $\ell(q,n,t) \geq q^{(t-1)(n-t-1)}$.*

Proof. By Theorem 2.1 and Lemma 2.4, we have

$$\ell(q,n,t) \geq \frac{q-1}{q^n-1}\binom{n}{t}_q = \frac{q-1}{q^n-1}\frac{(q^n-1)\cdots(q^{n-t+1}-1)}{(q^t-1)\cdots(q-1)} = \prod_{i=1}^{t-1}\frac{q^{n-t+i}-1}{q^{i+1}-1}.$$

However, $\dfrac{q^a-1}{q^b-1} \geq q^{a-b}$ whenever $a \geq b$; hence,

$$\ell(q,n,t) \geq \prod_{i=1}^{t-1} q^{n-t+i-(i+1)} = \prod_{i=1}^{t-1} q^{n-t-1} = q^{(t-1)(n-t-1)},$$

as claimed. □

We are also interested in studying the sum of the $\ell(q,n,t)$, as n is fixed and t varies, that is, in studying the number of orbits of $\mathcal{O}(L,F) = \mathcal{O}(\mathbb{F}_{q^n}, \mathbb{F}_q)$. Following the proof of Theorem 2.1, we can obtain the following formula:

$$\sum_{t=1}^{n} \ell(q,n,t) = \frac{1}{q^n-1}\left[\sum_{d|n}\left(\sum_{e|d}\mu\left(\frac{d}{e}\right)q^e\right)|\mathcal{O}(L,F_d)|\right] - \frac{1}{q^n-1}|\mathcal{O}(L,F)|,$$

where $F_d := \mathbb{F}_{q^d}$. However, the cardinality of $\mathcal{O}(L,F)$ can only be written as the sum of the q-binomial coefficients $\binom{n}{t}_q$, as t varies, and this expression cannot be further simplified. For this reason, we only give a bound for $\sum_{t=1}^{n}\ell(q,n,t)$. We denote by γ_n and c_n the integers defined as follows:

$$\gamma_n := \begin{cases} \frac{(n-2)^2}{4} & \text{if } n \text{ is even,} \\ \frac{(n-1)(n-3)}{4} & \text{if } n \text{ is odd;} \end{cases} \qquad c_n := \begin{cases} 1 & \text{if } n \text{ is even,} \\ 2 & \text{if } n \text{ is odd.} \end{cases}$$

Proposition 2.6. *Let q be a prime power and n be a positive integer. Then,*

$$\sum_{t=1}^{n}\ell(q,n,t) \le c_n q^{\gamma_n} + (2^n - c_n)q^{\gamma_n - 1} + 2^{n/2+1}\sqrt{n}\cdot q^{\gamma_n/2}.$$

Proof. By Theorem 2.1 and Lemma 2.4, we have

$$\ell(q,n,t) \le \frac{q-1}{q^n-1}\binom{n}{t}_q + \sum_{\substack{d|(n,t)\\ d\neq 1}} \frac{q^d-1}{q^n-1}\binom{n/d}{t/d}_{q^d}.$$

Hence, summing over t we have

$$\sum_{t=1}^{n}\ell(q,n,t) \le \sum_{t=1}^{n}\sum_{d|(n,t)}\frac{q^d-1}{q^n-1}\binom{n/d}{t/d}_{q^d} \le \sum_{d|n}\frac{q^d-1}{q^n-1}\sum_{s=1}^{n/d}\binom{n/d}{s}_{q^d} \le$$
$$\le \sum_{d|n}\frac{1}{q^{n-d}}\lambda\left(q^d,\frac{n}{d}\right),$$

where λ is defined as

$$\lambda(p,m) := \sum_{s=1}^{m}\binom{m}{s}_p := \sum_k T(m,k)p^k$$

for some coefficients $T(m,k)\in\mathbb{Q}$ (depending on m). Note that λ is a polynomial in p since each $\binom{m}{s}_p$ is a polynomial.

The degree of $\binom{m}{s}_p$ is $s(m-s)$; this quantity is maximal when $s=\lfloor m/2\rfloor$ or $s=\lceil m/2\rceil$. Hence, the degree of λ is equal to $\frac{m^2}{4}$ if m is even and $\frac{m^2-1}{4}$ if m is odd: call this number γ'_m. Each $\binom{m}{s}_p$ is monic (being the quotient of two monic polynomials) and thus the leading term of $\lambda(p,m)$ is 1 if m is even and 2 if m is odd; i.e., the leading term is c_m. Hence,

$$\lambda(p,m)=\sum_k T(m,k)p^k \leq c_m p^{\gamma'_m}+\left(\sum_k T(m,k)-c_m\right)p^{\gamma'_m-1}.$$

Since Gaussian binomial coefficients are defined for every $p>1$, so is $\lambda(p,m)$; when $p\to 1$, we have $\binom{m}{s}_p \to \binom{m}{s}$ and thus $\lambda(p,m)$ becomes exactly the sum of the binomial coefficients $\binom{m}{s}$ as s ranges from 1 to m: hence, the sum of the $T(m,k)$, as k varies, is equal to 2^m. Therefore,

$$\lambda(p,m)\leq c_m p^{\gamma'_m}+(2^m-c_m)p^{\gamma'_m-1}\leq 2^m p^{\gamma'_m}.$$

Using these inequalities, and dividing the case $d=1$ from the case $d\neq 1$, we have

$$\sum_{t=1}^{n}\ell(q,n,t)\leq \frac{1}{q^{n-1}}\left(c_n q^{\gamma'_n}+(2^n-c_n)q^{\gamma'_n-1}\right)+\sum_{\substack{d\mid n\\ d\neq 1}}\frac{1}{q^{n-d}}2^{n/d}q^{d(\gamma'_{n/d}-1)}.$$

When $d>1$, we have $d\gamma'_{n/d}\leq 2\gamma'_{n/2}\leq \frac{1}{2}\gamma'_n$; hence, since n has at most $2\sqrt{n}$ divisors, and since $\gamma_n=\gamma'_n-n+1$,

$$\sum_{t=1}^{n}\ell(q,n,t)\leq c_n q^{\gamma_n}+(2^n-c_n)q^{\gamma_n-1}+\sqrt{n}2^{n/2+1}q^{\gamma_n/2}.$$

This is exactly our claim. □

3. Star operations

Let $F\subseteq L$ be a field extension. We say that a map

$$\begin{aligned}\star\colon \mathcal{O}(L,F)&\longrightarrow \mathcal{O}(L,F)\\ V&\longmapsto V^\star\end{aligned}$$

is a *F-star operation on L* if, for every $V,W\in\mathcal{O}(L,F)$ and every $\beta\in L$, we have:

- $V\subseteq V^\star$;
- if $V\subseteq W$, then $V^\star\subseteq W^\star$;
- $(V^\star)^\star=V^\star$;
- $(\beta V)^\star=\beta\cdot V^\star$;
- $F^\star=F$.

We denote by $\mathrm{Star}_F(L)$ the set of F-star operations on L, and we endow this set with the partial order such that $\star_1\leq\star_2$ if and only if $V^{\star_1}\subseteq V^{\star_2}$ for every $V\in\mathcal{O}(L,F)$.

F-star operations are analogous to the star operations on integral domains: these are defined in the same way, except that the domain of definition is the set $\mathcal{F}(R)$ of the

nonzero fractional ideals of a domain R (a *fractional ideal* is an R-submodule I of the quotient field K such that $xI \subseteq R$ for some $x \in K$, $x \neq 0$), and $F^\star = F$ is substituted by the condition $R^\star = R$. In particular, there is a strong link between F-star operations and star operations defined on a pseudo-valuation domain: recall that R is a *pseudo-valuation domain* (in short, PVD) if it is a local domain such that its maximal ideal M is also the maximal ideal of a valuation overring V of R [5, Theorem 2.7]; V is called the valuation ring *associated* to R. More precisely, we have the following, which is implicitly present in [6] (especially in the proof of Theorem 2.5).

Theorem 3.1. *Let R be a PVD with associated valuation ring V, suppose $R \neq V$, and let F, L be the respective residue fields. Then, there is an order-preserving bijection between* $\mathrm{Star}(R)$ *and* $\mathrm{Star}_F(L)$.

Proof. Let $\pi : V \longrightarrow L$ be the quotient between V and the maximal ideal M. Then, π establishes a bijection between the set of fractional ideals I of R such that $R \subseteq I \subseteq V$ and the set $\mathcal{O}(L, F)$.

For every star operation $\star$ on R, we define $\Psi(\star) : \mathcal{O}(L, F) \longrightarrow \mathcal{O}(L, F)$ as the map such that

$$V^{\Psi(\star)} := \pi\left(\pi^{-1}(V)^\star\right).$$

It is easy to see that $\Psi(\star)$ is an F-star operation on L (note that $\pi^{-1}(F) = R$). Hence, the map $\Psi : \mathrm{Star}(R) \longrightarrow \mathrm{Star}(R)$ sending $\star$ to $\Psi(\star)$ is well-defined, and it is also clearly order-preserving.

Conversely, let $* \in \mathrm{Star}_F(L)$, and let I be a fractional ideal of R. If there is an $a \in K$ such that $R \subseteq aI \subseteq V$, define

$$I^{\Phi(*)} := a^{-1}\pi^{-1}\left(\pi(aI)^*\right);$$

otherwise, set $I^{\Phi(*)} = I$. It is clear that $I \subseteq I^\star$ and that $(I^\star)^\star = I^\star$ for every I (note that if $R \subseteq aI \subseteq V$ then $R \subseteq (aI)^{\Phi(*)} = aI^{\Phi(*)} \subseteq V$). Furthermore, $xI^{\Phi(*)} = (xI)^{\Phi(*)}$ and $R^\star = \pi^{-1}(F^*) = \pi^{-1}(F) = F$. To show that $\Phi(*)$ is a star operation on R, we thus have only to show that if $I \subseteq J$ then $I^{\Phi(*)} \subseteq J^{\Phi(*)}$.

If there is no a such that $R \subseteq aI \subseteq V$, then $I = I^{\Phi(*)}$ and the claim is clear. Suppose such an a exists. If also $R \subseteq aJ \subseteq V$, then by definition $I^{\Phi(*)} \subseteq J^{\Phi(*)}$. If not, then $V \subseteq aJ$ and so $I^{\Phi(*)} \subseteq a^{-1}V \subseteq J \subseteq J^{\Phi(*)}$. Hence, $\Phi(*)$ is a star operation on R and Φ is an order-preserving map $\mathrm{Star}_F(L) \longrightarrow \mathrm{Star}(R)$.

It is not hard to see that $\Phi \circ \Psi$ is the identity on $\mathrm{Star}_F(L)$; furthermore, $\Psi \circ \Phi$ is the identity since, if there is no a such that $R \subseteq aI \subseteq V$, then $I = I^\star$ for all $\star \in \mathrm{Star}(R)$ [6, Lemma 2.1]. Hence, $\mathrm{Star}(R)$ and $\mathrm{Star}_F(L)$ are order-isomorphic, as claimed. □

As a corollary, we have that when R is a PVD then $\mathrm{Star}(R)$ depends only on the extension $F \subseteq L$.

Corollary 3.2. *Let R, R' be two pseudo-valuation domains with associated valuation overring V, V', respectively, and suppose $R \neq V$, $R' \neq V'$. Let F, F' be the residue fields of R, R' and L, L' be the residue fields of V, V'. If there is a field isomorphism $\psi : L \longrightarrow L'$ such that $\psi(F) = F'$, then there is an order-preserving bijection $\Psi : \mathrm{Star}(R) \longrightarrow \mathrm{Star}(R')$.*

It is well-known that a star operation $\star$ can also be characterized by the set of the $\star$-*closed ideals*, that is, the ideals I such that $I = I^\star$; this set is denoted by $\mathcal{F}^\star(R)$. A set $\Delta \subseteq \mathcal{F}(R)$ is equal to $\mathcal{F}^\star(R)$ for some $\star \in \mathrm{Star}(R)$ if and only if the following hold: (a) $R \in \Delta$; (b) Δ is closed by intersections; (c) $xI \in \Delta$ for every $I \in \Delta$ and every $x \in K \setminus \{0\}$ (this essentially follows from [3, Proposition 32.4]). Translating these results to F-star operations, we have that there is a bijective correspondence between $\mathrm{Star}_F(L)$ and the family of subsets $\Lambda \subseteq \mathcal{O}(L, F)$ such that: (a) $F, L \in \Lambda$; (b) Λ is closed by intersections; (c) $\beta V \in \Lambda$ whenever $V \in \Lambda$ and $\beta \in L \setminus \{0\}$. We call a set with these properties a *star family*. In particular, if V is closed by $\star$ then all elements in the orbit of V under the action of L^* are closed. This suggests the following definition.

Definition 3.3. Let $\star \in \mathrm{Star}_F(L)$. The *level* of $\star$ is

$$\mathrm{lev}(\star) := \sup\{\dim_F W \mid W \subsetneq L, W = W^\star\}.$$

Since $F = F^\star$, the level of a star operation is always contained between 1 and $[L : F] - 1$.

Proposition 3.4. *Let $F \subseteq L$ be an extension of finite fields, with $|F| = q$ and $[L : F] = n$.*

(a) *There is a unique $\star \in \mathrm{Star}_F(L)$ of level 1.*
(b) *The unique F-star operation of level $n - 1$ is the identity.*
(c) *There are at least $2^{\ell(q,n,t)} - 1$ star operations of level t.*
(d) *There are exactly $2^{\ell(q,n,2)} - 1$ star operations of level 2.*

We note that part (b) is essentially a reformulation of [1, Theorem 1.14], while part (c) is essentially contained in the proof of [6, Theorem 2.5], and part (d) is basically contained in [6, Proposition 2.13].

Proof. (a) Suppose $\mathrm{lev}(\star) = 1$, and let Δ be the set of subspaces that are closed by $\star$. Then, $\Delta \subseteq \{F, L\} \cup \mathcal{O}_1(L, F)$; furthermore, every subspace V of dimension 1 is closed by every star operation (since $V = \alpha F$ for some α and F is closed); hence, the only possible Δ is exactly $\{F, L\} \cup \mathcal{O}_1(L, F)$. Moreover, this set is a star family, and thus there is exactly one star operation of level 1.

(b) If $\mathrm{lev}(\star) = n - 1$, there is an $(n-1)$-dimensional subset V that is $\star$-closed. Since $\ell(q, n, n-1) = 1$ (Corollary 2.2(c)), all subspaces of dimension $n-1$ are closed. However, every subspace W of L is the intersection of subspaces of codimension 1 (if $\beta \in L \setminus W$,

then there is always a subspace of codimension 1 containing V but not β, since there is always an hyperplane of L/V not containing $\beta+V$); therefore, every subspace is $\star$-closed, and thus $\star$ is the identity.

(c) Let Δ_0 be a nonempty set of orbits of the action of L^* on $\mathcal{O}_t(L,F)$, and let Δ be the set of the $V \in \mathcal{O}_t(L,F)$ such that the class of V is in Δ_0. Define Λ as the set composed by L, all αF, all $V \in \Delta$ and all intersections of elements of Δ; then, Λ is a star family, the star operation it is associated with has level t (no subspace of dimension $> t$ is contained in any $V \in \Delta$) and $\Lambda \cap \mathcal{O}_t(L,F) = \Delta$. Hence, every nonempty Δ_0 defines a different F-star operation of level t on L, and so we have at least $2^{\ell(q,n,t)} - 1$ star operations of level t.

(d) Suppose $\operatorname{lev}(\star) = 2$. Then, the one-dimensional subspaces are $\star$-closed; hence, $\star$ is determined by the set of 2-dimensional subspaces of L that are closed, and thus it is equal to one of the star operations found in the proof of (c). Hence, there are exactly $2^{\ell(q,n,2)} - 1$ star operations of level 2. □

Remark 3.5. The proof of the previous proposition partially works also when F is not finite, or when the degree $[L : F]$ is not finite. Indeed, part (a) always holds. Part (c) must be modified in the following way: for every nonempty set Y of orbits of $\mathcal{O}_t(L,F)$, let $\star_Y$ be the star operations generated by Y like in the proof. Then, the map $Y \mapsto \star_Y$ is an order-reversing embedding of the power set of $\mathcal{O}_t(L,F)$ (minus the empty set) into the set of star operations of level t. Likewise, part (d) will say that the set of star operations of level 2 is order-isomorphic to the power set of the set of the orbits of $\mathcal{O}_2(L,F)$.

We shall find in Section 4 a complete description of the set $\operatorname{Star}_F(L)$ when $[L : F] \leq 5$. Before doing so, we end this section by studying the asymptotic behavior of $|\operatorname{Star}_F(L)|$; to ease the notation, we denote by $\sigma(q,n)$ this cardinality when $|F| = q$ and $[L : F] = n$ (i.e., when $F = \mathbb{F}_q$ and $L = \mathbb{F}_{q^n}$). We first state a corollary of the previous proposition, which is a reformulation of [6, Theorem 2.5].

Corollary 3.6. *For all q, n, we have*

$$\left(\sum_{t=2}^{n-1} 2^{\ell(q,n,t)}\right) - n + 3 \leq \sigma(q,n) \leq 2^{\sum_{t=2}^{n-1} \ell(q,n,t)}.$$

Recall that γ_n and c_n were defined before Proposition 2.6.

Theorem 3.7. *Let $\epsilon > 0$. Then, the following hold.*

(a) *For every n there is a $q(\epsilon,n)$ such that, whenever $q \geq q(\epsilon,n)$,*

$$q^{\gamma_n} \leq \log_2 \sigma(q,n) \leq (c_n + \epsilon) q^{\gamma_n}$$

(b) *For every q there is a $n(\epsilon, q)$ such that, whenever $n \geq n(\epsilon, q)$,*

$$q^{\gamma_n} \leq \log_2 \sigma(q, n) \leq (1+\epsilon) q^{\gamma_n - 1 + n \log_q 2}.$$

Proof. By Corollary 3.6/[6, Theorem 2.5], we have $|\mathrm{Star}_F(L)| \geq 2^{\ell(q,n,m)}$, where $m := \lfloor n/2 \rfloor$; by Proposition 2.5, it follows that

$$\log_2 \sigma(q, n) \geq \ell(q, n, m) \geq q^{(m-1)(n-m-1)} = q^{\gamma_n}.$$

To prove the upper bounds, consider the inequality proved in Proposition 2.6. When n is fixed, the terms having degree in q less than γ_n become irrelevant; hence, $\ell(q, n, 2) + \cdots + \ell(q, n, n-1)$ becomes smaller than $(c_n + \epsilon) q^{\gamma_n}$ for large q, and (a) follows from Corollary 3.6.

Suppose now q is fixed. For large n, we have

$$\sqrt{n} \cdot 2^{n/2+1} q^{\gamma_n/2} \leq q^{n/2} q^{n/2+1} q^{\gamma_n}/2 \leq q^{\gamma_n - 1} \leq c_n q^{\gamma_n - 1};$$

hence, for large n we have

$$\sum_{t=1}^{n} \ell(q, n, t) \leq c_n q^{\gamma_n} + 2^n q^{\gamma_n - 1} \leq 2q^{\gamma_n} + q^{\gamma_n - 1 + n \log_q 2},$$

and so (b) follows. □

In particular, when n is fixed and even, then part (a) of the previous theorem implies that (using the big-O notation)

$$\log_2 \sigma(q, n) = q^{\gamma_n} + O_q(q^{\gamma_n - 1}).$$

It is unclear if a similar formula holds when n is odd (the constant of q^{γ_n} could be any number between 1 and 2, or it could be that $\log_2 \sigma(q, n)/q^{\gamma_n}$ does not have a limit); see Theorem 4.3 for the case $n = 5$.

4. Low degree

In this section, we analyze $\mathrm{Star}_F(L)$ when $[L : F] \leq 5$. The case $[L : F] = 1$ is trivial, while the cases $[L : F] = 2, 3$ were already in [6] (Theorems 2.3 and 2.6, respectively; we include them here for completeness), and the case $[L : F] = 4$ was only partially solved therein.

Proposition 4.1. *Let $F \subseteq L$ be a field extension.*

(a) *If $[L : F] \leq 2$, then $|\mathrm{Star}_F(L)| = 1$.*

(b) *If* $[L : F] = 3$, *then* $|\mathrm{Star}_F(L)| = 2$.
(c) *If* $[L : F] = 4$, *then* $|\mathrm{Star}_F(L)| = 2^{q+1} + 1$.

Proof. If $[L : F] = 1$ there is nothing to prove; if $[L : F] = 2$ then all F-star operations on L have level 1, and thus $|\mathrm{Star}_F(L)| = 1$ by Proposition 3.4(a).

If $[L : F] = 3$ and F is finite, then by Proposition 3.4 there is exactly one star operation of level 1 and one of level 2, and thus $|\mathrm{Star}_F(L)| = 2$. If F is not finite, then it is still true that all subspaces of codimension 1 are in the same orbit (see the proof of [6, Theorem 2.6]) and thus again there is a single star operation of level 2, and $|\mathrm{Star}_F(L)| = 2$.

Suppose $[L : F] = 4$. If F is infinite, then $|\mathrm{Star}_F(L)|$ is infinite by [6, Theorem 2.10]. If F is finite, then by Proposition 3.4 we have 1 star operation of level 1, $2^{\ell(q,n,2)} - 1$ of level 2 and 1 of level 3. By Theorem 2.1, we have

$$\begin{aligned}\ell(q,4,2) &= \frac{q-1}{q^4-1}\binom{4}{2}_q + \frac{1}{q^4-1}(\mu(2)q + \mu(1)q^2)\binom{2}{1}_{q^2} \\ &= \frac{q-1}{q^4-1}\frac{(q^4-1)(q^3-1)}{(q-1)(q^2-1)} + \frac{q^2-q}{q^4-1}\frac{(q^2)^2-1}{q^2-1} \\ &= \frac{q^3-1}{q^2-1} + \frac{q^2-q}{q^2-1} = q+1\end{aligned}$$

and the claim follows. □

Suppose from now on that $[L : F] = 5$ and that $|F| = q$ is finite. (If F is infinite, so is $\mathrm{Star}_F(L)$, again by [6, Theorem 2.10].) In this case, we have $\ell(q,5,2) = \ell(q,5,3) = q^2+1$. As in the previous proof, we have:

- 1 star operation of level 1;
- 1 star operation of level 4;
- $2^{\ell(q,5,2)} - 1 = 2^{q^2+1} - 1$ star operations of level 2.

Hence, we need to study the star operations of level 3.

Let V be a 2-dimensional subspace of L; since we are studying everything up to multiplication by elements of L, we can suppose without loss of generality that $1 \in V$, i.e., that $V = \langle 1, \alpha \rangle$ for some $\alpha \in L \setminus F$.

Let $\mathcal{W}$ be the set of 3-dimensional subspaces containing V. Clearly, $\mathcal{W}$ has the same cardinality of the set of 1-dimensional subspaces of a 3-dimensional vector space over F; that is, $|\mathcal{W}| = \binom{3}{1}_q = q^2 + q + 1$.

For every subspace W of L of dimension 3, there is a β such that $V \subseteq \beta W$: indeed, $W \cap \alpha^{-1}W$ cannot be $\{0\}$ (for dimensional reason), and thus if $\beta^{-1} \in W \cap \alpha^{-1}W$ then $\beta^{-1}, \alpha\beta^{-1} \in W$, and thus $\beta^{-1}V \subseteq W$, i.e., $V \subseteq \beta W$. This accounts for $q^2 + 1$ of the elements of $\mathcal{W}$, i.e., one for each class.

Consider now $Z := \langle 1, \alpha, \alpha^2 \rangle$; note that $\alpha^2 \notin \langle 1, \alpha \rangle$ since α has degree 5 over F. Clearly $V \subseteq Z$. Furthermore, for every $t \in F$, we have $(t+\alpha)V \subseteq Z$, that is, $V \subseteq \frac{1}{t+\alpha} Z =: Z_t$: indeed,

$$\begin{cases} 1 \cdot (t+\alpha) = t + \alpha \in Z \\ \alpha \cdot (t+\alpha) = t\alpha + \alpha^2 \in Z. \end{cases}$$

If $t \neq s$, then $Z_t \neq Z_s$, for otherwise $\frac{1}{t+\alpha} \in \frac{1}{s+\alpha} Z$, and thus

$$s + \alpha = (t+\alpha)(c_0 + c_1\alpha + c_2\alpha^2)$$

for some $c_0, c_1, c_2 \in F$, against the fact that α has degree 5 over F.

Therefore, the subspaces $Z, Z_0, \ldots, Z_{q-1}$ are $q+1$ distinct elements of $\mathcal{W}$, all belonging to the same orbit; $\mathcal{W} \setminus \{Z, Z_0, \ldots, Z_{q-1}\}$ has q^2 elements, and thus for cardinality reasons these elements are all nonequivalent one to each other, and neither are equivalent to Z.

Symmetrically, if W is a 3-dimensional subspaces, then the $q^2 + q + 1$ 2-dimensional subspaces contained in W can be divided in two parts: one containing $q+1$ subspaces, one equivalent to each other, and the other containing q^2 subspaces all nonequivalent, and all classes of 2-dimensional subspaces are represented between these subspaces.

Let now $\{[V_1], \ldots, [V_k]\}$ and $\{[W_1], \ldots, [W_k]\}$ be, respectively, the classes of 2-dimensional and 3-dimensional subspaces modulo multiplication by L^* (where $k := q^2 + 1$); we can order them in such a way that V_i is contained in $q+1$ subspaces equivalent to W_i.

Lemma 4.2. *Preserve the notation above, and let* $\star \in \mathrm{Star}_F(L)$.

(a) *If* W_i *is* $\star$*-closed, so is* V_i.
(b) *If* W_i, W_j *are* $\star$*-closed (with* $i \neq j$*) then every* V_l *is* $\star$*-closed.*

Proof. Take β_1, β_2 such that $V_i \subseteq \beta_1 W_i$ and $V_i \subseteq \beta_2 W_i$, and such that $\beta_1 W \neq \beta_2 W$. Then, $V_i = \beta_1 W_i \cap \beta_2 W_i$ is $\star$-closed. This proves (a).

To prove (b), let β_i, β_j such that $V_l \subseteq \beta_i W_i$, $V_l \subseteq \beta_j W_j$. If W_i and W_j are $\star$-closed, then so is $V_l = \beta_i W_i \cap \beta_j W_j$. □

In particular, we can distinguish two subclasses of star operations of level 3: star operations such that only one class of 3-dimensional subspaces is closed (we call them operations of the *first kind*) and star operations such that more than one class is closed (operations of the *second kind*).

Star operations of the second kind are easily counted: their number is equal to the number of subspaces of $\{[W_1], \ldots, [W_k]\}$ with at least two elements, that is, to

$$2^{q^2+1} - (q^2+1) - 1.$$

For the star operations of the first kind, we need an existence result. Indeed, let $\Delta_i := \{L\} \cup \{\beta F, \beta V_i, \beta W_i \mid \beta \in L^*\}$. Then, Δ_i is closed by multiplication and is also closed by intersections: the intersection between two βV_i, or between a βV_i and a γW_i, are either equal to βV_i or have dimension 1 (and thus are in the form βF). Similarly, the intersection between βW_i and γW_i have dimension 1 or are equal to $\beta' V_i$, and thus are in Δ_i. Hence, Δ_i is a star family corresponding to a star operation of the first kind that closes V_i but no other V_j.

Therefore, the star operations of the first kind that close W_i are in bijective correspondence with the subsets of $\{[V_1], \dots, [V_k]\} \setminus \{[V_i]\}$; thus, there are

$$(q^2+1)2^{q^2+1-1} = (q^2+1)2^{q^2}$$

star operations of the first kind. We have proved the following.

Theorem 4.3. *Let $F \subseteq L$ be a field extension with $|F| = q$ and $[L : F] = 5$. Then,*

$$|\mathrm{Star}_F(L)| = (q^2+1)(2^{q^2}-1) + 2^{q^2+2} = (q^2+5)2^{q^2} - (q^2+1).$$

Proof. It is enough to sum up the star operations of the various levels, i.e., calculate

$$|\mathrm{Star}_F(L)| = 1 + 2^{q^2+1} - 1 + (q^2+1)2^{q^2} + 2^{q^2+1} - (q^2+1) - 1 + 1$$

and then simplify the expression. □

In terms of the function σ defined in Section 3, this means that $\sigma(q,5) = (q^2+5)2^{q^2} - (q^2+1)$. Hence, it is not hard to see that

$$\log_2 \sigma(q,5) = q^2 + 2\log_2 q + o(1).$$

In particular, with regard to the remark after Theorem 3.7, for $n = 5$ the limit $(\log_2 \sigma(q,5))/q^2$ exists and is equal to 1.

References

[1] Valentina Barucci, Evan Houston, Thomas G. Lucas, Ira Papick, m-Canonical ideals in integral domains. II, in: Ideal Theoretic Methods in Commutative Algebra, Columbia, MO, 1999, in: Lecture Notes in Pure and Appl. Math., vol. 220, Dekker, New York, 2001, pp. 89–108.
[2] Paul-Jean Cahen, Jean-Luc Chabert, Integer-Valued Polynomials, Mathematical Surveys and Monographs, vol. 48, American Mathematical Society, Providence, RI, 1997.
[3] Robert Gilmer, Multiplicative Ideal Theory, Pure and Applied Mathematics, vol. 12, Marcel Dekker Inc., New York, 1972.
[4] R.L. Graham, M. Grötschel, L. Lovász (Eds.), Handbook of Combinatorics, vols. 1–2, Elsevier Science B.V./MIT Press, Amsterdam/Cambridge, MA, 1995.
[5] John R. Hedstrom, Evan G. Houston, Pseudo-valuation domains, Pac. J. Math. 75 (1) (1978) 137–147.
[6] Mi Hee Park, On the cardinality of star operations on a pseudo-valuation domain, Rocky Mt. J. Math. 42 (6) (2012) 1939–1951.
[7] Richard P. Stanley, Enumerative Combinatorics. Volume 1, second edition, Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012.