

Bounds on the number of ideals in finite commutative nilpotent $\mathbb{F}_p$ -algebras

By LINDSAY N. CHILDS (Albany) and CORNELIUS GREITHER (Neubiberg)

Abstract. Let A be a finite commutative nilpotent $\mathbb{F}_p$ -algebra structure on G , an elementary abelian group of order p^n . If K/k is a Galois extension of fields with Galois group G and $A^p = 0$, then corresponding to A is an H -Hopf Galois structure on K/k of type G . For that Hopf Galois structure we may study the image of the Galois correspondence from k -subHopf algebras of H to subfields of K containing k by utilizing the fact that the intermediate subfields correspond to the $\mathbb{F}_p$ -subspaces of A , while the subHopf algebras of H correspond to the ideals of A . We obtain upper and lower bounds on the proportion of subspaces of A that are ideals of A , and test the bounds on some examples.

Introduction

The motivation for this work is to understand the Galois correspondence for certain Hopf Galois structures on field extensions.

Let K/k be a Galois extension of fields with Galois group G . Then the Galois correspondence sending subgroups G' of G to subfields $K^{G'}$ of K containing k is, by the Fundamental Theorem of Galois Theory, a bijective correspondence from subgroups of G onto the intermediate fields between k and K .

In 1969, S. CHASE and M. SWEEDLER [CS69] defined the concept of a Hopf Galois extension of fields for a field extension K/k and H a k -Hopf algebra acting on K as an H -module algebra. They proved a weak version of the FTGT, namely, that there is an injective Galois correspondence from k -subHopf algebras H' of H to intermediate fields, given by $H' \mapsto K^{H'}$, the subfield of elements

Mathematics Subject Classification: 13M05, 16T05, 12F10.

Key words and phrases: nilpotent algebras, ideals, Hopf Galois theory.

fixed under the action of H' . But surjectivity was not obtained. GREITHER and PAREIGIS [GP87] defined a class of non-classical Hopf Galois structures, the “almost classical” structures, for which surjectivity holds, but also gave an example where it fails. Recent works of CRESPO, RIO and VELA ([CRV15] and especially [CRV16]) studied the image of the Galois correspondence for Hopf Galois structures on separable extensions K/k with normal closure $\tilde{K}$, and found numerous examples where surjectivity fails. In nearly all of the cases examined in [CRV16], the Galois group of $\tilde{K}/K$ is non-abelian.

In this paper, we seek to quantify the failure of the FTGT for Hopf Galois structures of the following type.

Let K/k be a Galois extension of fields with Galois group G , an elementary abelian p -group of order p^n . Suppose H is a k -Hopf algebra of type G (that means, $K \otimes_k H \cong KG$), and K/k is an H -Hopf Galois extension. As shown in [Ch15], [Ch16], [Ch17], building on work of [CDVS06] and [FCC12], every H -Hopf Galois structure of type G on a Galois extension of fields K/k with Galois group G , an elementary abelian p -group, arises from a commutative nilpotent $\mathbb{F}_p$ -algebra structure A on the additive group G with $A^p = 0$. In [Ch17], it was shown that the sub- k -Hopf algebras of H correspond to ideals of A . For a Galois extension K/k whose Galois group is an elementary abelian p -group (or equivalently, an $\mathbb{F}_p$ -vector space), the classical FTGT gives a bijection between $\mathbb{F}_p$ -subspaces of G and intermediate fields. So let $i(A)$ denote the number of ideals of A , and $s(A)$ the number of $\mathbb{F}_p$ -subspaces of A . Then the proportion of intermediate fields $k \subseteq E \subseteq K$ that are in the image of the Galois correspondence for an H -Hopf Galois structure on K/k arising from A is equal to $i(A)/s(A)$.

As observed in [Ch17], that comparison implies immediately that if $A^2 \neq 0$, then there are $\mathbb{F}_p$ -subspaces of A that are not ideals, and hence the Galois correspondence cannot be surjective.

Let e be the unique integer such that $A^e \neq 0$ and $A^{e+1} = 0$; we assume throughout that $e > 0$ (that is, A is not zero) and $e < p$. To quantify the failure of surjectivity of the FTGT for a Hopf Galois structure corresponding to A , we obtain in Section 2 of this paper a general upper bound, depending only on e , on the ratio $i(A)/s(A)$. The upper bound implies, for example, that for $e \geq 3$ and $p \geq 17$, $i(A)/s(A) < 0.01$.

Using information on the dimensions of the annihilator ideals of A , we obtain in Section 3 a lower bound on $i(A)$.

The upper bound is based on a lower bound on the fibers of the “ideal generated by” function G from subspaces of A to ideals of A . In the final section,

we examine that lower bound on fibers of G , and the inequalities of Sections 2 and 3, for some examples.

Let $s(n)$ denote the number of subspaces of an $\mathbb{F}_p$ -vector space of dimension n . Then $s(n)$ is a sum of Gaussian binomial coefficients, also called q -binomial coefficients (where $q = p$). The first section of the paper describes properties of these coefficients and obtains inequalities relating $s(m)$ and $s(n)$ for $m < n$.

Throughout the paper, we assume that A has dimension n and that $A^p = 0$. Recall that e is the largest number so that $A^e \neq 0$ (so $A^{e+1} = 0$). All vector spaces are over $\mathbb{F}_p$.

1. Gaussian binomial coefficients

To compare the number of ideals of a commutative nilpotent $\mathbb{F}_p$ -algebra A with the number of subspaces of A , we need to collect some information concerning the number of subspaces of dimension k of an $\mathbb{F}_p$ -vector space of dimension n . So we begin with Gaussian binomial coefficients.

The Gaussian binomial coefficient, or q -binomial coefficient (here $q = p$), is defined for $0 \leq k \leq n$ as

$$\begin{bmatrix} n \\ k \end{bmatrix} = \frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \cdots (p^k - p^{k-1})} = \frac{(p^n - 1)(p^{n-1} - 1) \cdots (p^{n-(k-1)} - 1)}{(p - 1)(p^2 - 1) \cdots (p^k - 1)},$$

and $\begin{bmatrix} n \\ k \end{bmatrix} = 0$ for $k > n$. It counts the number of k -dimensional subspaces of $\mathbb{F}_p^n$. So

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ n - k \end{bmatrix} \text{ for all } k, \quad \begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1.$$

Then

$$s(n) = \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix}$$

is the total number of subspaces of $\mathbb{F}_p^n$. Note that it suffices to replace the factors $(p^n - p^r)/(p^k - p^r)$ by p^n/p^k in order to see that

$$\begin{bmatrix} n \\ k \end{bmatrix} \geq p^{k(n-k)},$$

and that $\begin{bmatrix} n \\ k \end{bmatrix}$ has order of magnitude $p^{k(n-k)}$ for large p .

(In fact, the rational function

$$\begin{bmatrix} n \\ k \end{bmatrix}_x = \frac{(x^n - 1)(x^n - x) \cdots (x^n - x^{k-1})}{(x^k - 1)(x^k - x) \cdots (x^k - x^{k-1})}$$

is a polynomial of degree $(n-k)k$ in $\mathbb{Z}[x]$. For let $b(x), a(x)$ be the numerator and denominator of $\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_x$. Both are monic polynomials in $\mathbb{Z}[x]$. Dividing $b(x)$ by $a(x)$ in $\mathbb{Q}[x]$ gives

$$b(x) = a(x)q(x) + r(x),$$

where $\deg(r(x)) < \deg(a(x))$. Since $a(x)$ is monic, $q(x)$ and $r(x)$ are in $\mathbb{Z}[x]$. Now $b(p)/a(p) = \left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right]_p$ is a positive integer for every prime p , so the rational function $r(p)/a(p)$ is also an integer for every prime p . But

$$\lim_{p \rightarrow \infty} \frac{r(p)}{a(p)} = 0.$$

So $r(p) = 0$ for all primes greater than some fixed bound, and hence $r(x) = 0$. So $b(x)/a(x) = q(x)$ is in $\mathbb{Z}[x]$.

The Gaussian binomial coefficients satisfy two recursive formulas, analogous to that satisfied by the usual binomial coefficients:

$$\left[\begin{smallmatrix} n \\ k \end{smallmatrix}\right] = \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right] + p^k \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right] = p^{n-k} \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix}\right].$$

Using properties of the Gaussian binomial coefficients, we will now obtain some inequalities relating the number of subspaces of $\mathbb{F}_p$ -vector spaces of dimensions $n, n-1$ and $n-2$ for all n .

Let

$$\delta(n) = \left\lfloor \frac{n^2}{4} \right\rfloor = \begin{cases} n^2/4, & \text{if } n \text{ is even,} \\ (n^2-1)/4, & \text{if } n \text{ is odd.} \end{cases}$$

Lemma 1.1.

- (a) For all $n \geq 2$, we have $s(n) \geq p^{n-1}s(n-2)$.
- (b) If $n > 1$ is even, then $s(n) \geq \frac{1}{2}p^{n/2}s(n-1)$.
- (c) If $n > 0$ is odd, then $s(n) \geq p^{(n-1)/2}s(n-1)$.
- (d) For $n \geq m \geq 0$ arbitrary, we have $s(n) \geq \frac{1}{2}p^{\delta(n)-\delta(m)}s(m)$. The factor $1/2$ may be omitted if m and n have the same parity or if n is odd.

PROOF. (a) Using the two recursion formulas for $\left[\begin{smallmatrix} n \\ d \end{smallmatrix}\right]$, in turn we find:

$$\begin{aligned} \left[\begin{smallmatrix} n \\ d \end{smallmatrix}\right] &= \left[\begin{smallmatrix} n-1 \\ d-1 \end{smallmatrix}\right] + p^d \left[\begin{smallmatrix} n-1 \\ d \end{smallmatrix}\right] \\ &= \left[\begin{smallmatrix} n-1 \\ d-1 \end{smallmatrix}\right] + p^d \left(p^{n-1-d} \left[\begin{smallmatrix} n-2 \\ d-1 \end{smallmatrix}\right] + \left[\begin{smallmatrix} n-2 \\ d \end{smallmatrix}\right] \right) \geq p^{n-1} \left[\begin{smallmatrix} n-2 \\ d-1 \end{smallmatrix}\right]. \end{aligned}$$

Summing these for $d = 1, \dots, n-1$ gives the required inequality.

(b) Let $n = 2k$. We may calculate as follows:

$$\begin{aligned} s(n) &\geq \begin{bmatrix} n \\ 1 \end{bmatrix} + \dots + \begin{bmatrix} n \\ k \end{bmatrix} = \left(p^{n-1} \begin{bmatrix} n-1 \\ 0 \end{bmatrix} + \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \right) \\ &\quad + \left(p^{n-2} \begin{bmatrix} n-1 \\ 1 \end{bmatrix} + \begin{bmatrix} n-1 \\ 2 \end{bmatrix} \right) + \dots + \left(p^k \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + \begin{bmatrix} n-1 \\ k \end{bmatrix} \right) \\ &\geq p^k \begin{bmatrix} n-1 \\ 0 \end{bmatrix} + p^k \begin{bmatrix} n-1 \\ 1 \end{bmatrix} + \dots + p^k \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} = p^k s(n-1)/2. \end{aligned}$$

(c) Let $n = 2k+1$. Using one recursive formula, then the other, we get:

$$\begin{aligned} \begin{bmatrix} n \\ 1 \end{bmatrix} &\geq p^{n-1} \begin{bmatrix} n-1 \\ 0 \end{bmatrix} \geq p^k \begin{bmatrix} n-1 \\ 0 \end{bmatrix}, \\ \begin{bmatrix} n \\ 2 \end{bmatrix} &\geq p^{n-2} \begin{bmatrix} n-1 \\ 1 \end{bmatrix} \geq p^k \begin{bmatrix} n-1 \\ 1 \end{bmatrix}, \\ &\vdots \\ \begin{bmatrix} n \\ k-1 \end{bmatrix} &\geq p^{n-(k-1)} \begin{bmatrix} n-1 \\ k-2 \end{bmatrix} \geq p^k \begin{bmatrix} n-1 \\ k-2 \end{bmatrix}; \end{aligned}$$

(now we switch to the other recursive formula)

$$\begin{aligned} \begin{bmatrix} n \\ k \end{bmatrix} &\geq p^k \begin{bmatrix} n-1 \\ k \end{bmatrix}, \\ \begin{bmatrix} n \\ k+1 \end{bmatrix} &\geq p^{k+1} \begin{bmatrix} n-1 \\ k+1 \end{bmatrix}, \\ \begin{bmatrix} n \\ k+2 \end{bmatrix} &\geq p^{k+2} \begin{bmatrix} n-1 \\ k+2 \end{bmatrix} \geq p^k \begin{bmatrix} n-1 \\ k+2 \end{bmatrix}, \\ &\vdots \\ \begin{bmatrix} n \\ n-1 \end{bmatrix} &\geq p^{n-1} \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} \geq p^k \begin{bmatrix} n-1 \\ n-1 \end{bmatrix}. \end{aligned}$$

Now observe that

$$\begin{bmatrix} n-1 \\ k+1 \end{bmatrix} = \begin{bmatrix} 2k \\ k+1 \end{bmatrix} = \begin{bmatrix} 2k \\ k-1 \end{bmatrix}.$$

Therefore

$$p^{k+1} \begin{bmatrix} n-1 \\ k+1 \end{bmatrix} \geq p^k \left(2 \begin{bmatrix} n-1 \\ k+1 \end{bmatrix} \right) = p^k \left(\begin{bmatrix} n-1 \\ k+1 \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \right).$$

Thus $s(n)$ is at least as large as the sum of the left sides of the inequalities, which is at least the sum of the right sides of the inequalities, and in view of the last observation, the sum of the right sides is at least $p^k s(n-1)$.

(d) We first note that $\delta(n) - \delta(n-2) = n-1$, so by (a),

$$s(n) \geq p^{n-1} s(n-2) = p^{\delta(n)-\delta(n-2)} s(n-2).$$

Iterating this shows that if $n > m$ and $n \equiv m \pmod{2}$, then

$$s(n) \geq p^{\delta(n)-\delta(m)} s(m).$$

If n is even and m is odd, then $n/2 = \delta(n) - \delta(n-1)$, and by (b) we find

$$s(n) \geq \frac{1}{2} p^{\frac{n}{2}} s(n-1) = \frac{1}{2} p^{\delta(n)-\delta(n-1)} s(n-1),$$

so

$$s(n) \geq \frac{1}{2} p^{\delta(n)-\delta(m)} s(m).$$

If n is odd and m is even, then $(n-1)/2 = \delta(n) - \delta(n-1)$, so by (c),

$$s(n) \geq p^{\frac{n-1}{2}} s(n-1) = p^{\delta(n)-\delta(n-1)} s(n-1),$$

hence

$$s(n) \geq p^{\delta(n)-\delta(m)} s(m). \quad \square$$

2. An upper bound on the number of ideals of A

In this section, we obtain a general upper bound for the ratio $i(A)/s(A)$ of the number of ideals of A to the number of subspaces of A , for A an arbitrary commutative nilpotent $\mathbb{F}_p$ -algebra of dimension n . To do so, we consider the function G from subspaces of A to ideals of A which associates to each subspace U the ideal $G(U) = U + AU$ generated by U , and we establish a lower bound on the cardinality of the fiber of each ideal under this map (which is obviously surjective). But first, we need to count subspaces with certain properties.

Recall that $\delta(t) = \lfloor t^2/4 \rfloor$. All vector spaces are over $\mathbb{F}_p$, and the number of k -dimensional subspaces of W , an $\mathbb{F}_p$ -vector space of dimension d , is $\begin{bmatrix} d \\ k \end{bmatrix}$.

We show:

Proposition 2.1. *Let $\dim(W) = d$, and let W_0 be a fixed subspace of W of dimension r . For $k \leq d - r$, the number $s(d, r; k)$ of k -dimensional subspaces U of W with $U \cap W_0 = (0)$ is equal to p^{rk} times the number of k -dimensional subspaces of W/W_0 :*

$$s(d, r; k) = p^{rk} \begin{bmatrix} d - r \\ k \end{bmatrix}.$$

PROOF. Let V be a complementary subspace to W_0 , so that $V \oplus W_0 = W$. For $k \leq d - r$, let U be a k -dimensional subspace of V , with basis $(z_1, \dots, z_k)$. For each choice $\bar{a} = (a_1, \dots, a_k)$ of elements of W_0 , the subspace $U_{\bar{a}}$ of W generated by $(z_1 + a_1, \dots, z_k + a_k)$ is k -dimensional and has trivial intersection with W_0 . For suppose

$$c_1(z_1 + a_1) + \dots + c_k(z_k + a_k) = a$$

in W_0 for some $c_1, \dots, c_k$ in $\mathbb{F}_p$. Then, since $V \oplus W_0$ is a direct sum of $\mathbb{F}_p$ -vector spaces,

$$c_1 z_1 + \dots + c_k z_k = 0.$$

Since $z_1, \dots, z_k$ are linearly independent, $c_1, \dots, c_k = 0$, hence $a = 0$. The same argument with $a = 0$ shows that $(z_1 + a_1, \dots, z_k + a_k)$ is a linearly independent set.

Finally, each choice of elements $\bar{a} = (a_1, \dots, a_k)$ of W_0 gives a different subspace $U_{\bar{a}}$ of A . For suppose $z_i + b_i$ is in the space $U_{\bar{a}}$. Then

$$z_i + b_i = c_1(z_1 + a_1) + \dots + c_i(z_i + a_i) + \dots + c_k(z_k + a_k).$$

So

$$0 = c_1(z_1 + a_1) + \dots + ((c_i - 1)z_i + c_i a_i - b_i) + \dots + c_k(z_k + a_k).$$

But then

$$0 = c_1 z_1 + \dots + (c_i - 1)z_i + \dots + c_k z_k.$$

So $c_i = 1$, all other $c_j = 0$, and the equation reduces to

$$a_i - b_i = 0.$$

Thus for each k -dimensional subspace U of W , we obtain p^{rk} k -dimensional subspaces $U_{\bar{a}}$ of W with $U \cap W_0 = (0)$. $\square$

Corollary 2.2. *Let W be a t -dimensional space and $W_0 \subset W$ a subspace of codimension 1. Then the number of subspaces of W not contained in W_0 is at least $p^{\delta(t)}$.*

PROOF. First we remark that via a duality argument, the number of subspaces of dimension k not contained in a fixed subspace of codimension 1 is the same as the number of subspaces of dimension $t - k$ intersecting a fixed subspace of dimension 1 trivially. Hence the preceding proposition is applicable; summing over all possible dimensions of U , we find that the number of subspaces $U \subset W$ not contained in W_0 is

$$\begin{aligned} s(t, 1) &:= \sum_{k=0}^{t-1} s(t, 1; k) = \sum_{k=0}^{t-1} p^k \begin{bmatrix} t-1 \\ k \end{bmatrix} \\ &\geq \sum_{k=0}^{t-1} p^k p^{k(t-1-k)} = \sum_{k=0}^{t-1} p^{k(t-k)} \geq p^{\lfloor \frac{t^2}{4} \rfloor} = p^{\delta(t)}. \end{aligned} \quad \square$$

Recall that G is the map from subspaces of A to ideals of A defined by

$$G(V) = V + AV.$$

To simplify notation, we write $G(S)$ instead of $G(\langle S \rangle_{\mathbb{F}_p})$ for any subset S of A . To get a sense of the relationship between the number of subspaces of A and the number of ideals of A , we will count the number of elements in the fibers of G .

Assume $e > 0$ is minimal with $A^{e+1} = 0$. (The zero algebra $A = 0$ can be safely excluded from our study.) Consider the chain

$$N_1 \subset N_2 \subset \cdots \subset N_e = A$$

of annihilator ideals defined by

$$N_k := \text{Ann}_k(A) = \{a \in A \mid x_1 x_2 \cdots x_k a = 0 \text{ for all } x_1, \dots, x_k \text{ in } A\}.$$

Let $\dim_{\mathbb{F}_p}(N_k) = d_k$. Then the sequence $(d_k)_k$ is obviously increasing, and a little argument shows that $0 < d_1 < d_2 < \cdots < d_e = n$.

The strategy for bounding the number of ideals of A begins with the following idea. Let $\mathcal{J}_t$ be the set of ideals J of A contained in N_t but not contained in N_{t-1} . Then, since N_t is an ideal of A for all t , we have

$$\sum_{J \in \mathcal{J}_t} |G^{-1}(J)| = s(N_t) - s(N_{t-1}).$$

The next lemma will help us find a lower bound on $|G^{-1}(J)|$.

Lemma 2.3. *Let $W = G(\{x\}) = \mathbb{F}_p x + Ax$, $W_0 = Ax$ as above. Let U be a subspace of W , not contained in W_0 . Then $G(U) = W$.*

PROOF. Let y be in U , y not in W_0 . Then $G(\{y\}) \subseteq G(U)$. After multiplying y by a non-zero element of $\mathbb{F}_p$, we can assume that $y = x - ax$ for some a in A . Then

$$y + ay + a^2y + \cdots + a^{e-1}y = x$$

is in $G(\{x\})$. So

$$W = G(\{x\}) \subseteq G(\{y\}) \subseteq G(U) \subseteq W.$$

□

Let J be an ideal of A of $\mathbb{F}_p$ -dimension d , let $s(J)$ (or $s(d)$) be the number of subspaces of J , and let $i(J)$ be the number of ideals of A that are contained in J . Lemma 2.3 enables us to prove a result relating the number of subspaces and the number of ideals contained in the annihilator ideal N_t in A for each t .

Proposition 2.4. *For each t with $1 \leq t \leq e$, consider the ideal map G restricted to the set of subspaces V of N_t that are not contained in N_{t-1} . For each x in $N_t \setminus N_{t-1}$, let $q(x) = \dim(G(x))$, and let $q_t = \min_{x \in N_t \setminus N_{t-1}} q(x)$. Then for all ideals J in $\mathcal{J}_t$,*

$$|G^{-1}(J)| \geq p^{\delta(q_t)}.$$

Hence

$$p^{\delta(q_t)} (i(N_t) - i(N_{t-1})) \leq s(N_t) - s(N_{t-1}).$$

PROOF. Let J be an ideal contained in N_t , not contained in N_{t-1} . Let x be in J , x not in N_{t-1} . Let $W_0 = Ax$ and $W = G(\{x\}) = \mathbb{F}_p x + Ax$. Then W has dimension at least q_t , and W_0 has codimension 1 in W . Let Y be a complement of W in J . Then for every subspace U of W not contained in W_0 , we have $G(U) = W$, and thus $G(U + Y) = J$.

Whenever U and U' are distinct subspaces of W not contained in W_0 , we have $U + Y \neq U' + Y$. So the number of preimages of $J = G(\{x\} + Y)$ is at least equal to the number of subspaces of W that are not contained in W_0 . Since $\dim(W) \geq q_t$, that number of subspaces is $\geq p^{\delta(q_t)}$ by Corollary 2.2. □

Dividing both sides of the t -th inequality of Proposition 2.4 by $p^{\delta(q_t)}$ and summing them over all t yields an upper bound for the number of ideals of A :

Corollary 2.5.

$$i(A) \leq \sum_{t=1}^{e-1} (p^{-\delta(q_t)} - p^{-\delta(q_{t+1})}) s(N_t) + p^{-\delta(q_e)} s(N_e).$$

Omitting the negative terms and applying Lemma 1.1 (d) yields the following upper bound on $i(A)$ in terms of $s(A)$ (recall $d_t = \dim N_t$):

Corollary 2.6.

$$i(A) \leq \left(\sum_{t=1}^{e-1} 2p^{-\delta(q_t)+\delta(d_t)-\delta(d_e)} + p^{-\delta(q_e)} \right) s(A).$$

To make it easier to apply this inequality for general A , we show the following simple lower bound on the quantity q_t . (Recall it was defined by $q_t = \min_{x \in N_t \setminus N_{t-1}} q(x)$ with $q(x) = \dim(G(x))$.)

Proposition 2.7. *For all $t > 0$, we have $q_t \geq t$.*

PROOF. This is clear for $t = 1$.

For $t > 1$, let x be in N_t and not in N_{t-1} . Let $u_1, u_2, \dots, u_{t-1}$ in A so that $u_1 u_2 \cdots u_{t-1} x \neq 0$. Then for each k , $x_k = u_k \cdots u_{t-1} x$ is in N_k and not in N_{k-1} . So $x_1, \dots, x_{t-1}, x$ are linearly independent in A . Thus $G(x) = \mathbb{F}_p x + Ax$ has dimension at least t . $\square$

In the next theorem, we will use this lower bound on q_t to get a general, fairly elegant upper bound on $i(A)/s(A)$ that only depends on e , the length of the annihilator chain in A . However, in some of the examples treated below, it will be worthwhile to have a closer look at q_t ; we will find it to be considerably larger than t , which will enable us to sharpen the upper bound.

The general bound goes as follows.

Theorem 2.8. *With the above hypotheses on A and e , we have*

$$\frac{i(A)}{s(A)} \leq \frac{2e-1}{p^{\delta(e)}}.$$

PROOF. In the inequality of Corollary 2.6, replace q_t by t and observe that since $1 < d_1 < d_2 < \cdots < d_e$, one has $\delta(d_e) - \delta(d_t) \geq \delta(e) - \delta(t)$. If we insert this into the inequality, the terms $p^{\pm\delta(t)}$ cancel and we obtain

$$i(A) \leq \sum_{t=1}^{e-1} 2p^{-\delta(e)} s(N_e) + p^{-\delta(e)} s(N_e) = (2e-1)p^{-\delta(e)} s(A). \quad \square$$

For $e = 2, 3$, the inequalities of Theorem 2.8 are

$$i(A) \leq \frac{3}{p} s(A) \quad \text{for } e = 2; \quad i(A) \leq \frac{5}{p^2} s(A) \quad \text{for } e = 3.$$

We can improve these bounds by some constant factors, (almost) without imposing further conditions on the algebra A . Recall that $n = \dim(A)$ and $e < p$.

Proposition 2.9. *For $e = 2$, we have*

$$i(A) \leq \frac{2}{p}s(A),$$

whenever $p \geq 3$ and $n \geq 3$. For $e = 3$, we have

$$i(A) \leq \frac{2}{p^2}s(A),$$

whenever $p \geq 5, n \geq 4$.

PROOF. *Case $e = 2$.* From Corollary 2.5 with $\delta(q_t)$ replaced by $\delta(t)$, we have

$$i(A) \leq \left(1 - \frac{1}{p}\right)s(N_1) + \frac{1}{p}s(A).$$

To get the claimed inequality, it suffices to assume that $\dim N_1 = n - 1$, and show that

$$\left(1 - \frac{1}{p}\right)s(n - 1) \leq \frac{1}{p}s(n),$$

or $(p - 1)s(n - 1) \leq s(n)$. Using Lemma 1.1 (b) for n even, it suffices to show that

$$\frac{p^{n/2}}{2} > p - 1,$$

which holds for $p \geq 3, n \geq 4$, while for n odd, it suffices by Lemma 1.1 (c) to show that

$$p^{(n-1)/2} > p - 1,$$

which holds for $p \geq 3, n \geq 3$.

Case $e = 3$. From Corollary 2.5, we have

$$i(A) \leq \left(1 - \frac{1}{p}\right)s(N_1) + \left(\frac{1}{p} - \frac{1}{p^2}\right)s(N_2) + \frac{1}{p^2}s(A).$$

Since $s(A) = s(n)$, the right side is maximized when $s(A) = s(n)$, $s(N_2) = s(n - 1)$, $s(N_1) = s(n - 2)$. To show that the right side is $\leq \frac{2}{p^2}s(A)$, it suffices to show that

$$\left(1 - \frac{1}{p}\right)s(n - 2) + \left(\frac{1}{p} - \frac{1}{p^2}\right)s(n - 1) \leq \frac{1}{p^2}s(n).$$

Using Lemma 1.1 (a) and Lemma 1.1 (b) for n even, we are reduced to showing that

$$\left(1 - \frac{1}{p}\right)\frac{1}{p^{n-1}} + \left(\frac{1}{p} - \frac{1}{p^2}\right)\frac{2}{p^{n/2}} \leq \frac{1}{p^2},$$

which holds for $p \geq 3$, $n \geq 4$. Similarly, using Lemma 1.1 (c) for n odd, we see it suffices to show that

$$\left(1 - \frac{1}{p}\right) \frac{1}{p^{n-1}} + \left(\frac{1}{p} - \frac{1}{p^2}\right) \frac{1}{p^{(n-1)/2}} \leq \frac{1}{p^2},$$

which holds for $n \geq 5$ and $p \geq 2$. $\square$

The bounds of Theorem 2.8 and Proposition 2.9 imply:

Corollary 2.10. *Suppose K/k is a Galois extension with elementary abelian p -group G and is also an H -Hopf Galois extension where H arises from a commutative nilpotent $\mathbb{F}_p$ -algebra structure A on the additive group G , where $A^e \neq 0$, $A^{e+1} = 0$ and $e < n \leq p$. Then $i(A)/s(A)$ is the proportion of intermediate fields that are in the image of the Galois correspondence from sub-Hopf algebras of H , and $i(A)/s(A) < 0.01$ for*

$$e = 2, p \geq 200, \quad e = 3, p \geq 17, \quad e = 4, p \geq 7,$$

all e, p with $5 \leq e < p$.

The case $e = n$ is the “uniserial” case of Example 4.1 below and [Ch17, Theorem 4.2]. For uniserial algebras,

$$\frac{i(A)}{s(A)} = \frac{e+1}{s(e)} \leq \frac{e+1}{p^{\lfloor \frac{e^2}{4} \rfloor}} \leq 0.01$$

for

$$e = 2, p \geq 300, \quad e = 3, p \geq 20,$$

all p, e with $4 \leq e < p$.

3. A lower bound on the number of ideals

We now obtain a lower bound on the number of ideals of A , by exhibiting a collection of ideals in A and estimating its size. Recall that $A^e \neq 0 = A^{e+1}$ and that we defined

$$N_r = \text{Ann}_r(A) = \{a \in A \mid x_1 x_2 \cdots x_r a = 0 \text{ for all } x_1, \dots, x_r \text{ in } A\}.$$

Then N_r is an ideal of A , and

$$(0) \subset N_1 \subset N_2 \subset \cdots \subset N_e = A,$$

all inclusions being proper.

We already defined $d_r = \dim(N_r)$; let us put $t_r = \dim_{\mathbb{F}_p}(N_r/N_{r-1})$. For each $r = 1, \dots, e$, let W_r be a subspace of A so that

$$N_r = W_r \oplus N_{r-1}.$$

(In particular, $W_1 = N_1$.) Then $t_r = \dim(W_r)$,

$$A = W_1 \oplus W_2 \oplus \dots \oplus W_e$$

and

$$t_1 + t_2 + \dots + t_e = n.$$

Proposition 3.1.

$$i(A) \geq \lambda(A) := s(t_1) + (s(t_2) - 1) + \dots + (s(t_e) - 1).$$

PROOF. For each r , $1 \leq r \leq e$, and each non-zero subspace V_r of W_r , let $J = N_{r-1} + V_r$. Then J is an ideal of A . Indeed, we have $AV_r \subset AN_r \subset N_{r-1}$, and therefore $AJ \subset AN_{r-1} + N_{r-1} \subset N_{r-1} \subset J$.

The formula $\lambda(A)$ of the proposition simply counts the number of ideals J just described. $\square$

Since for any m ,

$$s(m) = \sum_{k=0}^m \begin{bmatrix} m \\ k \end{bmatrix}$$

and $\begin{bmatrix} m \\ k \end{bmatrix} \geq p^{(m-k)k}$, we can let $t_M = \max t_k$, and get a rough lower bound for the number of ideals in A :

$$i(A) \geq p^{\delta(t_M)}.$$

4. Some classes of examples

To see how sharp the bounds on ideals are that we obtained in the last two sections, we look at some explicit classes of algebras.

Example 4.1. First, consider the “uniserial” e -dimensional algebra A generated by x with $x^{e+1} = 0$. In this case, for every element u in $N_t \setminus N_{t-1}$, the dimension $q(x) = \dim(G(\{x\}))$ is equal to t . We then see that the general upper bound

$$i(A) \leq (2e - 1)p^{-\delta(e)}s(A)$$

is in fact close to the true number $i(A) = e + 1$ for large p , since $s(A)$ is a polynomial in p of degree $\delta(e)$.

The lower bound $\lambda(A)$ in this simple class of examples is $e + 1$.

Example 4.2. Let A be a “binomial” nilpotent algebra: $A = \langle x_1, x_2, \dots, x_e \rangle$ with $x_k^2 = 0$ for all k . Then $\dim(A) = 2^e - 1$, $\text{Ann}(A) = (x_1 x_2 \cdots x_e)$ and $\dim(N_t/N_{t-1}) = \binom{e}{t-1}$.

Theorem 2.8 tells us that the ratio of ideals to subspaces for A is bounded as follows:

$$\frac{i(A)}{s(A)} \leq \frac{2e-1}{p^{\delta(e)}} = \frac{2e-1}{p^{\lfloor \frac{e^2}{4} \rfloor}}.$$

But that inequality arose from minorizing $q_t = \min_{x \in N_t \setminus N_{t-1}} \dim(G(x))$ by t throughout. In this class of examples we can do better, having a closer look at q_t .

Proposition 4.3. *Let A be the binomial algebra of dimension $2^e - 1$. Then for every non-zero u in $N_t \setminus N_{t-1}$, we have*

$$\dim(G(u)) \geq 2^{t-1}.$$

PROOF. For any given u in $N_t \setminus N_{t-1}$, pick a monomial summand y of u in $N_t \setminus N_{t-1}$. Renumber the variables of A so that

$$y = x_1 x_2 \cdots x_{e-t+1}.$$

Then we introduce an ordering on the set of all nonzero monomials of A so that any monomial of N_{k-1} comes after any monomial of $N_k \setminus N_{k-1}$ for all k , and the monomials within $N_k \setminus N_{k-1}$ are ordered lexicographically. Strictly speaking, this is a total ordering on the set of all monomials up to multiplication with a nonzero scalar in $\mathbb{F}_p$.

Call a family of monomials admissible if no two of them are equal up to a nonzero scalar. Every nonzero $z \in A$ has a unique “leading” monomial $m(z)$, according to the ordering. The following is easy to see: if $(z_i)_{i \in I}$ is a family of elements of A , such that the family of leading monomials $(m(z_i))_i$ is admissible, then $(z_i)_i$ is $\mathbb{F}_p$ -linearly independent. If w is any monomial, then we have $m(zw) = m(z)w$, unless $m(z)w$ happens to be zero, in which case nothing much can be said about $m(zw)$.

Now consider the family F of monomials that consist only of factors $x_{e-t+2}, \dots, x_e$; this family has 2^{t-1} entries, and is of course admissible. If we recall that y is the leading term of u and look at the family of products $uF = \{u\xi \mid \xi \in F\}$, then, since $y\xi$ is never zero, we see that the leading term of $u\xi$ is $y\xi$, and these again form an admissible family. Hence the elements of the family uF are linearly independent, which shows that the ideal $G(u)$ generated by u has dimension at least 2^{t-1} . $\square$

We illustrate how working with $q_t \geq 2^{t-1}$ instead of the crude lower bound $q_t \geq t$ affects the upper bound on the ratio $i(A)/s(A)$ of Theorem 2.8 for a binomial algebra.

Consider the binomial algebra $A = \langle x_1, x_2, x_3, x_4 \rangle$ with $x_i^2 = 0$. Then

$$\dim(N_1) = 1, \dim(N_2) = 5, \dim(N_3) = 11, \dim(N_4) = 2^4 - 1 = 15.$$

(Note $N_4 = A$.) The general inequality 2.8 gives

$$\frac{i(A)}{s(A)} \leq \frac{7}{p^4}.$$

Let us start afresh. From Corollary 2.5, we have

$$i(A) \leq \sum_{t=1}^3 (p^{-\delta(q_t)} - p^{-\delta(q_{t+1})}) s(N_t) + p^{-\delta(4)} s(A).$$

Omitting the negative terms gives

$$i(A) \leq \frac{1}{p^{\delta(q_1)}} s(N_1) + \frac{1}{p^{\delta(q_2)}} s(N_2) + \frac{1}{p^{\delta(q_3)}} s(N_3) + \frac{1}{p^{\delta(q_4)}} s(N_4).$$

Now $\delta(q_1) = \delta(1) = 0$ and for $t > 1$, $\delta(q_t) \geq \delta(2^{t-1}) = 2^{t-4}$. So we have

$$i(A) \leq s(1) + \frac{1}{p} s(5) + \frac{1}{p^4} s(11) + \frac{1}{p^{16}} s(15).$$

Now we use Lemma 1.1 (d):

$$\begin{aligned} s(15) &\geq p^{\delta(15)-\delta(1)} s(1) = p^{56} s(1); & s(15) &\geq p^{\delta(15)-\delta(5)} s(5) = p^{50} s(5); \\ s(15) &\geq p^{\delta(15)-\delta(11)} s(11) = p^{26} s(11). \end{aligned}$$

So

$$\frac{i(A)}{s(A)} \leq \left(\frac{1}{p^{56}} + \frac{1}{p^{51}} + \frac{1}{p^{30}} + \frac{1}{p^{16}} \right) \leq \frac{2}{p^{16}}.$$

This is a big improvement over the inequality above that comes from the general approach.

However, the lower bound $\lambda(A)$ on the number of ideals of A from Proposition 3.1 is a polynomial in p of degree 9, while

$$\frac{2}{p^{16}} s(15) > \frac{2}{p^{16}} \begin{bmatrix} 15 \\ 7 \end{bmatrix} > \frac{2}{p^{16}} p^{56} = 2p^{40}.$$

So there remains a large gap between the upper and lower bounds on $i(A)$.

In general, the gap between the upper and lower bounds for $i(A)$ arises because the upper bound is based on a lower bound on the sizes of fibers of the ideal generator map

$$G : (\text{subspaces of } A) \rightarrow (\text{ideals of } A).$$

For J an ideal of N_k , not in N_{k-1} , we showed that $|G^{-1}(J)| \geq p^{\delta(q_k)}$, where q_k is the minimum of the dimensions of *principal* ideals $G(x)$ for x in $N_k \setminus N_{k-1}$. But for many nilpotent algebras A and many ideals J of A , this lower bound greatly underestimates $|G^{-1}(J)|$. We illustrate this with two examples.

Example 4.4. Let A be the “triangular” algebra $A = \langle x, y \rangle$ with $A^{e+1} = 0$. Here one sees that $q(u) = \frac{t(t+1)}{2}$ for all u in $N_t \setminus N_{t-1}$, hence $q_t = \frac{t(t+1)}{2}$. Let us look at the case $e = 2$ in detail.

Let $A = \langle x, y \rangle$ with $A^3 = 0$. Then A has a basis $\mathcal{B} = (x, y, x^2, xy, y^2)$, and the annihilator $N_1 = \text{Ann}(A)$ has basis x^2, xy, y^2 . Moreover $N_2 = A$. So we have $d_1 = 3$ and $d_2 = 5$.

Proposition 4.5. *There are $3p^2 + 4p + 6$ ideals in A .*

PROOF. The lower bound $\lambda(A)$ from Proposition 3.1 counts ideals of N_1 and ideals of A properly containing N_1 : that number is

$$\begin{aligned} \lambda(A) &= s(t_1) + s(t_2) - 1 = s(3) + s(2) - 1 \\ &= (2p^2 + 2p + 4) + (p + 2) = 2p^2 + 3p + 6. \end{aligned}$$

To determine the number of ideals of A , we let $\bar{A} = A/N_1$. This is the two-dimensional algebra spanned by $\bar{x}$ and $\bar{y}$ with zero multiplication. We classify ideals $J \subset A$ by their image $\bar{J}$ in $\bar{A}$. Those with $\bar{J} = 0$ are simply the subspaces of N_1 , which we have already counted. One easily sees that $\bar{J} = \bar{A}$ only happens once, for $J = A$, and since that ideal contains N_1 , it is already counted.

There remains the case where $\bar{J}$ is one-dimensional. There are $p + 1$ one-dimensional subspaces of $\bar{A}$, but by applying suitable automorphisms of A it suffices to count ideals with $\bar{J} = \mathbb{F}_p \bar{x}$, and multiply that count by $p + 1$. All such J contain x^2 and xy , so the question is whether they contain y^2 . If yes, J is simply the linear span of x and N_1 and has been counted. If no, then J contains an element $x + ay^2$ for a unique scalar $a \in \mathbb{F}_p$; this scalar determines the ideal. So there are p such ideals mapping onto $\mathbb{F}_p \bar{x}$. Thus the count of ideals J with $\bar{J}$ one-dimensional is $p(p + 1)$. Adding that number to $\lambda(A)$ gives the result. $\square$

We can write down all of the ideals explicitly and determine their fibers. The notation (m) denotes “subspace generated by m ”. In the list, a, b, d are arbitrary elements of $\mathbb{F}_p$.

$$\begin{aligned} A &= G(x, y) \\ J_1 &= J_1(a, d) = G(x + ay + dy^2) = (x + ay + dy^2, x^2 - a^2y^2, xy + ay^2) \\ J_{15} &= J_{15}(a) = G(x + ay, y^2) = (x + ay, x^2, xy, y^2) \\ J_2 &= J_2(b) = G(y + bx^2) = (y + bx^2, xy, y^2) \\ J_{23} &= G(y, x^2) = (y, x^2, xy, y^2), \\ \text{and finally all subspaces of the ideal } N_1 &= (x^2, xy, y^2). \end{aligned}$$

To describe the subspaces of A , choose the basis (x, y, x^2, xy, y^2) of A . Looking at row vectors of coordinates with respect to that basis yields a bijection between subspaces of A and row spaces of 5×5 matrices with entries in $\mathbb{F}_p$. Those row spaces are in bijective correspondence with the set of 5×5 reduced row echelon matrices. Those, in turn, can be categorized by specifying the columns where the pivots occur: the number of pivots specified defines the dimension of the subspace. Thus the label (124) denotes the 5×5 reduced row echelon matrix

$$\begin{pmatrix} 1 & 0 & \cdot & 0 & \cdot \\ 0 & 1 & \cdot & 1 & \cdot \\ 0 & 0 & 0 & 1 & \cdot \end{pmatrix}$$

(we omit all rows of zeros), where the five unspecified entries can be arbitrary elements of $\mathbb{F}_p$. Thus there are p^5 subspaces of A corresponding to echelon forms with label (124).

The echelon forms (3), (4), (5), (34), (35), (45), (345) define the non-zero subspaces of N_1 . Those subspaces are also ideals of A since multiplication on $N_1 = \text{Ann}(A)$ is trivial.

Every echelon form that includes both 1 and 2 defines a subspace of A that generates the ideal A . It is possible to discuss all other forms in turn, finding the ideals generated by the corresponding subspaces and the exact size of the fiber of G . Since this is repetitive and space-consuming, we only write out what happens for three echelon forms.

(1) has the form $(1, a', b', c', d')$ and generates $J_1(a, d)$ for $a = a'$ and $d = d' + b'a'^2 - c'a'$. So for each (a, d) there are p^2 subspaces of type (1) that generate $J_1(a, d)$.

(13) has the form $\begin{pmatrix} 1 & a' & 0 & c' & d' \\ 0 & 0 & 1 & e' & f' \end{pmatrix}$. If $a' = a$, $d' - c'a + e'a^2 = d$ and $f' = e'a - a^2$, then it generates $J_1(a, d)$. In that case, for each (a, d) , there are p^2 subspaces of type (13) that generate $J_1(a, d)$. If $a' = a$ and $f' \neq e'a - a^2$, then the subspace generates $J_{15}(a)$. In that case, the choices for (c', d', e', f') yield $p^3(p-1)$ subspaces of type (13) that generate $J_{15}(a)$.

(14) has the form $\begin{pmatrix} 1 & a' & b' & 0 & d' \\ 0 & 0 & 0 & 1 & f' \end{pmatrix}$. If $f' = a' = a$, then the subspace generates $J_1(a, d)$ for all p choices of b' ; otherwise for $a' = a \neq f'$, there are $p^2(p-1)$ choices of (b', d', f') for subspaces of type (14) that generate $J_{15}(a)$.

As noted, we omit the (easy) discussion of the remaining forms (134), (1345), (135), (145), (15), (2), (23), (234), (2345), (235), (24), (245), (25).

Adding up the number of subspaces that generate each ideal, we get the tables below. Here a, b, d are arbitrary elements of $\mathbb{F}_p$.

ideals	# of ideals	fiber size
A	1	$2p^6 + p^5 + 2p^4 + p^3 + p^2 + 1$
$J_1(a, d)$	p^2	$2p^2 + p + 1$
$J_{15}(a)$	p	$p^4 + p^3 + p^2 + 1$
$J_2(b)$	p	$2p^2 + p + 1$
J_{23}	1	$p^4 + p^3 + p^2 + 1$
ideal of N_1	$2p^2 + 2p + 4$	1

The center column sums to the number of ideals of A .

The total number of subspaces of A accounted for by fibers of ideals of each type is:

ideals	# subspaces
A	$2p^6 + p^5 + 2p^4 + p^3 + p^2 + 1$
$J_1(a, c)$	$2p^4 + p^3 + p^2$
$J_{15}(a)$	$p^5 + p^4 + p^3 + p$
$J_2(b)$	$2p^3 + p^2 + p$
J_{23}	$p^4 + p^3 + p^2 + 1$
ideal of N_1	$2p^2 + 2p + 4$

The right column sums to $s(5)$ = the number of subspaces of A .

Let us compare this with our more general results. We have

$$s(5) = 2p^6 + 2p^5 + 6p^4 + 6p^3 + 6p^2 + 4p + 6.$$

Given that $i(A) = 3p^2 + 4p + 6$ by Proposition 4.5, the inequality of Proposition 2.9 comes out as

$$3p^2 + 4p + 6 \leq 4p^5 + 4p^4 + 12p^3 + 12p^2 + 12p + 8 + 12p^{-1}.$$

This inequality was based on assuming that every ideal J not contained in N_1 has dimension ≥ 2 , and so $|G^{-1}(J)| \geq p^{\delta(2)} = p$.

In Corollary 2.6, the factor in brackets between $\leq$ and $s(A)$ evaluates to $2p^{-4} + p^{-2}$, using $d_1 = 3, d_2 = 5$ and $q_1 = 1, q_2 = 3$. This assumed that every ideal J not contained in N_1 has dimension ≥ 3 , so $|G^{-1}(J)| \geq p^{\delta(3)} = p^2$. Then the inequality is

$$3p^2 + 4p + 6 \leq 2p^4 + 2p^3 + 10p^2 + 10p + 18 + r(p),$$

where $r(p) = 12p^{-4} + 8p^{-3} + 18p^{-2} + 16p^{-1}$ is always positive but tends to 0 for $p \rightarrow \infty$.

Looking at the actual sizes of the fibers of G in this example, the inequality $|G^{-1}(J)| \geq p^2$ has the correct power of p for principal ideals J . But the non-principal ideals J_{23} , $J_{15}(a)$ and A that are not contained in N_2 have fibers with cardinalities of order p^4, p^4 and p^6 , respectively. This helps explain why the general upper bound on ideals is loose.

Example 4.6. Let $A = \langle x, y, z \rangle$ with $x^2 = y^2 = z^2 = 0$, the binomial algebra in three variables. Then $A^4 = 0$ ($e = 3$), and A has a basis

$$(x, y, z, xy, xz, yz, xyz)$$

with $N_1 = (xyz)$, $N_2 = (xy, xz, yz, xyz)$. The number of subspaces of A is:

$$s(7) = 2p^{12} + 2p^{11} + 6p^{10} + 8p^9 + \text{terms in } p \text{ of lower degree}.$$

The lower bound on $i(A)$, the number of ideals of A , is

$$\lambda(A) = s(1) + (s(3) - 1) + (s(3) - 1) = 4p^2 + 4p + 8.$$

For $p \geq 3$, the number of ideals of A turns out to be

$$i(A) = 7p^2 + 4p + 8.$$

(Sketch of argument: Given $\lambda(A)$, we only need to count the number of ideals of A not contained in N_2 and not containing N_2 : these are exactly the principal ideals Aw generated by elements

$$w := ax + by + cz + dxy + exz + fyz + gxyz,$$

where one or two of a, b, c are zero. Indeed, if none of a, b, c is zero, then the ideal Aw contains N_2 and therefore is already accounted for; if all three are zero, the Aw is contained in N_2 , and, again, already counted. Looking at the echelon forms of the ideals Aw yields $3p^2$ ideals.)

An upper bound on $i(A)$ can be obtained by using Proposition 4.3, which says that the dimension of a principal ideal of A not contained in N_2 is at least 4. Then we get

$$\begin{aligned} i(A) &\leq \left(\frac{1}{p^{\delta(7)-\delta(1)}} + \frac{2}{p \cdot p^{\delta(7)-\delta(4)}} + \frac{1}{p^4} \right) s(A) \\ &= \left(\frac{1}{p^{12}} + \frac{2}{p^9} + \frac{1}{p^4} \right) s(A) \leq \frac{2}{p^4} s(A) \sim 4p^8 + 2p^7 + \dots \end{aligned}$$

To see why this upper bound on $i(A)$ is off by a factor of a constant times p^6 , we can determine $|G^{-1}|$ for the ideals of A , by methods in the last example. We omit the details. But we observe first that the fibers of the $2p^2 + 3p + 4$ ideals of N_2 account in total for $s(4) = p^4 + 3p^3 + 4p^2 + 3p + 5$ subspaces of A . So most subspaces of A generate ideals not contained in N_2 .

In obtaining our upper bound, we used that for principal ideals of A not contained in N_2 , $|G^{-1}(J)| \geq p^4$. But in fact, we find that:

For the $p^2 + p + 1$ principal ideals J of the form $G(x + by + cz)$ with $bc \neq 0$ in $\mathbb{F}_p$, the dimension of $J \geq p^5$, so $|G^{-1}(J)| \geq p^{\delta(5)} = p^6$, not p^4 . Thus this set of ideals is generated by approximately p^8 subspaces of A .

For the $p^2 + p + 1$ non-principal ideals of the form

$$G(x + bz, y + cz), \quad G(x + by, z), \quad G(y, z),$$

each is generated by at least p^9 subspaces of A . Thus this set of ideals is generated by approximately p^{11} subspaces of A .

Finally, for the ideal $A = G(x, y, z)$ itself, every subspace of A whose reduced row echelon form has the form $(123\dots)$ generates A , and summing the number of such subspaces yields

$$|G^{-1}(A)| \geq 2p^{12} + p^{11} + 2p^{10} + 2p^9 + \dots$$

Comparing that to $s(7) = s(A)$ above, it is evident that the weakness in the upper bound we found for $i(A)$ arises from the considerable underestimation of the size of $G^{-1}(J)$ for non-principal ideals not contained in N_2 , and, in particular, on the size of $G^{-1}(A)$: $|G^{-1}(A)|$ is a polynomial in p of the same degree as $s(A)$.

This last fact turns out to be true in general. One can show (proof omitted) that $|G^{-1}(A)|$ is always a polynomial in p with the same degree as the polynomial $s(A)$, under the fairly mild assumption that A as an $\mathbb{F}_p$ -algebra is generated by at most $\dim(A)/2$ elements.

From these examples, it appears that any substantial tightening of the upper bound for the ideals of A will require a more nuanced look at the fibers of non-principal ideals whose $\mathbb{F}_p$ -dimension is close to the dimension of A .

However, the primary objective of this paper has been achieved. Let L/K be a Galois extension with elementary abelian Galois group an elementary abelian p group G . If L/K is an H -Hopf Galois extension of type G corresponding to a commutative nilpotent algebra structure A on G with $A^p = 0$, then the upper bound on $i(A)/s(A)$ in Section 2, weak as it may be for some examples, still provides the first general quantitative estimate on how far from surjective is the Galois correspondence for the Hopf Galois structure on L/K .

ACKNOWLEDGEMENTS. Our thanks go to the University of Nebraska at Omaha and to GRIFF ELDER for their hospitality and support, and to the referees for their careful reading of the manuscript.

References

- [CDVS06] A. CARANTI, F. DALLA VOLTA and M. SALA, Abelian regular subgroups of the affine group and radical rings, *Publ. Math. Debrecen* **69** (2006), 297–308.
- [CS69] S. U. CHASE and M. E. SWEEDLER, Hopf Algebras and Galois Theory, Lecture Notes in Mathematics, Vol. **97**, Springer-Verlag, Berlin – New York, 1969.
- [Ch15] L. N. CHILDS, On abelian Hopf Galois structures and finite commutative nilpotent rings, *New York J. Math.* **21** (2015), 205–229.
- [Ch16] L. N. CHILDS, Obtaining abelian Hopf Galois structures from finite commutative nilpotent rings, arXiv:1604.05269.
- [Ch17] L. N. CHILDS, On the Galois correspondence for Hopf Galois structures, *New York J. Math.* **23** (2017), 1–10.
- [CRV15] T. CRESPO, A. RIO and M. VELA, From Galois to Hopf Galois: theory and practice, In: Trends in Number Theory, *Contemp. Math.* **649**, American Mathematical Society, Providence, RI (2015), 29–46.
- [CRV16] T. CRESPO, A. RIO and M. VELA, On the Galois correspondence theorem in separable Hopf Galois theory, *Publ. Mat.* **60** (2016), 221–234.
- [FCC12] S. C. FEATHERSTONHAUGH, A. CARANTI and L. N. CHILDS, Abelian Hopf Galois structures on prime-power Galois field extensions, *Trans. Amer. Math. Soc.* **364** (2012), 3675–3684.

516 L. N. Childs and C. Greither : Bounds on the number of ideals...

[GP87] C. GREITHER and B. PAREIGIS, Hopf Galois theory for separable field extensions,
J. Algebra **106** (1987), 239–258.

LINDSAY N. CHILDS
DEPARTMENT OF MATHEMATICS
UNIVERSITY AT ALBANY
1400 WASHINGTON AVENUE
ALBANY, NY 12222
USA

E-mail: lcchilds@albany.edu

CORNELIUS GREITHER
FAKULTÄT INFORMATIK
UNIVERSITÄT DER
BUNDESWEHR MÜNCHEN
WERNER-HEISENBERG-WEG 39
85579 NEUBIBERG
GERMANY

E-mail: cornelius.greither@unibw.de

(Received July 7, 2017; revised September 20, 2017)