On the Galois correspondence ratio for Hopf-Galois extensions arising from nilpotent $\mathbb{F}_p$-algebras

Lindsay N. Childs

June 7, 2023

The Galois Correspondence Ratio

Suppose L/K is a G-Galois extension of fields with an H-Hopf-Galois structure of type N, where $L \otimes_K N \cong L[N]$. The Galois correspondence ratio $GCR(L/K, G, N)$ is

$$= \frac{\#\{\text{fields } K \subseteq E \subset L \text{ fixed by a sub-Hopf algebra of } H\}}{\#\{\text{fields } K \subseteq E \subset L\}}.$$

and measures the failure of surjectivity of the Galois correspondence for the H-Galois structure on L/K. Such an extension L/K defines a left skew brace $(B, *, \circ)$ with $G \cong (B, \circ)$ and $N \cong (B, *)$, then

$$GCR(L/K, G, N) = i(B)/s(B, \circ)$$

where $i(B)$ is the number of left ideals of B and $s(B, \circ) = s(G)$ is the number of subgroups of the Galois group $G(B, \circ)$.

Previous result I

This talk involves nilpotent $\mathbb{F}_p$-algebras and is related to three results. One is the result of L. Stefanello and S. Trappeniers, [ST22] that if $B(*, \circ)$ is a biskew brace, thereby yielding two GCR's,
one on a $(B, \circ)$-Galois extension of fields with an Hopf-Galois structure of type $(B, *)$,
the other a $(B, *)$-Galois extension with a Hopf-Galois structure of type $(B, \circ)$,
then the ratio of the two GCR's is equal to the ratio $s(B, *)/s(B, \circ)$ of the numbers of subgroups of $(B, *)$ and $(B, \circ)$. (This follows immediately from their result that the left ideals of the two brace structures on B are the same.)

Previous result II

The second is the main theorem of [CG18]. Let A be a commutative nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$-dimension n, e is the smallest number so that $A^{e+1} = 0$ and $e < p$. Let L/K be a G-Galois extension and an H-Hopf-Galois extension where $G = (A, \circ)$ and H has type $(A, +)$. Then the GCR,

$$GCR(L/K, G, N) = \frac{i(A)}{s(A, \circ)} \leq \frac{2e+1}{p^{\delta(e)}}$$

where $\delta(e) = \lfloor \frac{e^2}{4} \rfloor$.

Previous result III

The third is an example I presented here in 2017: let
$A = A_{1,e} = \mathbb{F}_p[x]/(x^{e+1})$. Then $i(A) = e + 1$ and $s(A) = s(\mathbb{F}_p^e) \sim p^{\delta(e)}$.
So the GCR goes to 0 with increasing p or e.
I want to generalize this rxample.

Nilpotent $\mathbb{F}_p$-algebras

A nilpotent $\mathbb{F}_p$-algebra A has exponent e if $A^e \neq 0$ and $A^{e+1} = 0$, where A^r is the subalgebra generated by all products of r elements of A. The circle operation $\circ$ defined by $a \circ b = a + b + ab$ makes $(A, \circ)$ a group, where the inverse of a in A is $\overline{a} = -a + a^2 - a^3 + \ldots$. Then $(A, +, \circ)$ into a left skew brace, and the left ideals of A coincide with the left ideals of the left skew brace A.
Given a nilpotent $\mathbb{F}_p$-algebra A and a G-Galois extension L/K of fields where $G \cong (A, \circ)$, then L/K has a H-Hopf-Galois structure where H has type $N \cong (A, +)$.

Results

I want to present two results. The first relates to the result of [ST22] just noted:

•If A is a nilpotent $\mathbb{F}_p$-algebra, then the number of subgroups of $(A, \circ)$ = the number of subgroups of $(A, +)$. So the denominator of the GCR is known. In particular, $(A, +, \circ)$ is a bi-skew brace iff $A^3 = 0$, and in that case the two GCR's are equal.

The second is a generalization of the 2017 example $A(1, e)$:

•Let $A = A(n, e)$ be the nilpotent $\mathbb{F}_p$-algebra on n generators subject only to the relation $A^{e+1} = 0$. If L/K is a $(A, \circ)$-Galois extension with an H-Hopf-Galois structure of type $(A, +)$, then the GCR goes to 0 with increasing p, e or n.

Subgroups of the circle group of a nilpotent $\mathbb{F}_p$-algebra

Let A be a finite nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$ dimension n with multiplication $\cdot$ (often omitted). Then $a \circ b = a + b + ab$, and the $\circ$-inverse of a, $\overline{a}, = -a + a^2 - a^3 - \ldots$.
Let A^i be the ideal of A generated over $\mathbb{F}_p$ by all products $a_1 \cdot a_2 \cdot \ldots \cdot a_i$ for $a_1, \ldots, a_i$ in A. Then $(A^i, \circ)$ is a normal subgroup of $(A, \circ)$, and for a, b in A^i, $a \circ b = a + b + c$ for c in A^{i+1}, so i9s addition modulo A_{i+1}, and for any positive integer r,
$a^{\circ r} = a \circ a \circ \ldots \circ a = ra +$ (element of A^{i+1}), hence is scalar multiplication by r modulo A_{i+1}.

Elementary linear algebra

So choose a basis of A, $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \ldots \cup \mathcal{B}_e$, where $\mathcal{B}_i$ is a lift to A^i of a basis of A^i/A^{i+1}, where $\circ = +$. Given any $\circ$-subgroup S of $(A, \circ)$, we pick a $\circ$-generating set $\mathcal{G}_S$ of S, and write the elements of $\mathcal{G}_S$ as $\mathbb{F}_p$-linear combinations of the basis vectors of $\mathcal{B}$.

Elementary row operations

Form the matrix M with n columns whose rows consist of the $\mathcal{B}$-coordinates of the vectors in $\mathcal{G}_S$. Then, starting from the rows that have non-zero components of the basis vectors $\mathcal{B}_1$, we can use the circle operations $a \circ b$ and $a^{\circ s}$, which modulo A^2 are the same as addition and scalar multiplication by s, as elementary row operations to get the columns of M corresponding to $\mathcal{B}_1$ into reduced row echelon form (RREF), obtaining the matrix M_1.

Then repeat with the rows that have no non-zero components of $\mathcal{B}_1$ to get the columns of M_1 corresponding to $\mathcal{B}_2$ (and hence also of $\mathcal{B}_1$) into RREF (observing that a $\circ$-row operation involving adding a multiple of a vector with no A_1 components to a vector with A_1 components will not change those A_1-components).

RREF

Call the resulting matrix M_2. Etc. Proceeding from left to right, as one typically does for any matrix in elementary linear algebra, the result is a matrix $M = M_e$ in RREF whose rows are a $\circ$-basis of the $\circ$-subgroup S of $(A, \circ)$. Each RREF matrix M has a sequence of rows with pivots (leading ones). Let $n(M)$ be the number of matrix entries in the columns without pivots and to the right of leading ones. For example, if

$$M = \begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}$$

then $n(M) = 3$, and $p^{n(M)} = p^3$ is the number of subgroups (subspaces) with the given pivot sequence (relative to the basis $\mathcal{B}$). .

Counting subspaces

We thus have, just as in elementary linear algebra:
Every subgroup of $(A, \circ)$ has a unique RREF M, and the number of subgroups with a given RREF is equal to $p^{n(M)}$ where $n(M)$ is the number of parameters (free variables) in the RREF M.
The total number of subgroups of $(A, \circ)$ is then the sum of the $p^{n(M)}$ over all possible RREF's M.
But this will be true whether the RREF's are obtained by addition and scalar multiplication of row vectors (which for matrices of elements of $\mathbb{F}_p$ can be obtained by addition of row vectors), or by the circle operation. So:

Theorem

Let A be a finite nilpotent $\mathbb{F}_p$-algebra. Then the number of subgroups of $(A, \circ)$ is equal to the number of subgroups of $(A, +)$.

Counting subspaces

Corollary

Let A be a nilpotent $\mathbb{F}_p$-algebra of $\mathbb{F}_p$-dimension n, n even. Then the number of subgroups of $(A, \circ)$ is asymptotic to $p^{n^2/4}$ for large n.

For it is evident that if n is even, then the RREF with n columns with the most parameters is the RREF with $n/2$ rows and leading ones in the leftmost $n/2$ columns, hence has $(\frac{n}{2})^2$ parameters.
(If n is odd, then the two RREF's with the most parameters are the ones with leading ones in the leftmost $(n-1)/2$ and leftmost $(n+1)/2$ columns, and each has $(n-1)(n+1)/4$ parameters.)

The algebra $A(n, e)$

Let $A = A_{n,e}$ be the $\mathbb{F}_p$-algebra $A = \mathbb{F}_p[x_1, x_2, \ldots, x_n]/A^{e+1}$: that is, the free non-commutative $\mathbb{F}_p$-algebra on $x_1, ...x_n$ subject only to the relations $A^e = 0$. As an $\mathbb{F}_p$-vector space, it has dimension $d = n + n^2 + n^3 + \ldots + n^e$. The algebra $A_{1,e}$ was discussed earlier. For $A = \mathbb{F}_p[x_1, x_2, \ldots, x_n]$ with $A^{e+1} = 0$, we pick the basis $\mathcal{B}$ of A of which the first n vectors are $x_1, x_2, \ldots, x_n$, a basis of A mod A^2; the next n^2-vectors are $x_1x_1, x_2x_1, \ldots, x_nx_1, x_1x_2, x_2x_2, x_3x_2, ...x_nx_n$, a basis of A^2 mod A^3,etc. The columns of the corresponding $\mathbb{F}_p$ matrix will be denoted by the subscripts of corresponding basis vectors.
Can we estimate the number of ideals of A by determining RREF's of ideals?

The RREF of an ideal

Suppose J is a left ideal of A. Then if v is in J then so are bv for every basis vector in $\mathcal{B}$. This property imposes a restriction on the possible pivot sequences for an ideal:
Suppose the ideal $(J + A^2)/A^2$ has dimension r_1, $((J \cap A^2) + A^3)/A^3$ has dimension r_2, etc. If v is an element of J, then so are $x_1 v, x_2 v, \ldots, x_n v$. So the RREF for J will have r_1 leading ones in the columns $1, 2, \ldots, n$; $nr_1 + r_2$ leading ones in the columns $11, 12, \ldots, nn$; $n^2 r_1 + nr_2 + n_3$ leading ones in the columns $111, 112, \ldots, nnn$; etc. For

$$M = \begin{pmatrix} 1 & c & 0 & 0 & 0 & * \\ 0 & 0 & 1 & 0 & c & 0 \\ 0 & 0 & 0 & 1 & 0 & c \\ 0 & 0 & 0 & 0 & 1 & * \end{pmatrix},$$

$n = 2, r_1 = r_2 = 1$.

The RREF of an ideal, ctd.

$$M = \begin{pmatrix} 1 & c & 0 & 0 & 0 & * \\ 0 & 0 & 1 & 0 & c & 0 \\ 0 & 0 & 0 & 1 & 0 & c \\ 0 & 0 & 0 & 0 & 1 & * \end{pmatrix},$$

$(n = 2, r_1 = r_2 = 1)$.
It is clear that given RREF matrices with m leading ones, the matrix with the most free parameters is the one where the m leading ones are as far to the left as possible.
So among the RREF matrices for left ideals of A, the matrix with the most free parameters will have pivots in the first r_1 columns of A, in the first $nr_1 + r_2$ columns of A^2, the first $n^2r_1 + nr_2 + n_3$ columns of A^3, etc.

The RREF of an ideal, ctd.

$$M = \begin{pmatrix} 1 & c & 0 & 0 & 0 & * \\ 0 & 0 & 1 & 0 & c & 0 \\ 0 & 0 & 0 & 1 & 0 & c \\ 0 & 0 & 0 & 0 & 1 & * \end{pmatrix}$$

The free parameters for such a matrix contains parameters in the rightmost $n - r_1$ columns of the A/A^2 part of the matrix, the rightmost $n^2 - nr_1 - r_2$ columns of the A^2/A^3 part of the matrix, etc. The number of rows that can have free parameters are r_1 in the A/A^2 part of the matrix, $r_1 + nr_1 + r_2$ in the A^2/A^3 part of the matrix, etc. But the parameters in nr_1 of those rows are not new–they are repeats of the parameters in the portion of the A_1-portion of the matrix.
So the maximal number of parameters for an ideal is

$$M := (n - r_1)(r_1) + (n^2 - nr_1 - r_2)(r_1 + r_2) + \ldots$$

Counting parameters of an ideal

Continuing this process, given an ideal J and a basis $\mathcal{B}$ of J chosen so that r_i of the basis vectors are in $J \cap A^i$ for each $1 \leq i \leq e$, then the maximal number of parameters for such a J is

$$M = \sum_{k=1}^{e} M_i,$$

where for all $1 \leq i \leq e$,

$$M_i = (n^i - n^{i-1}r_1 - \ldots - nr_{i-1} - r_i)(r_1 + \ldots + r_i)$$

and

$$0 \leq n^{i-1}r_1 + n^{i-2}r_2 + \ldots + nr_{i-1} + r_i \leq n^i.$$

An upper bound on the number of parameters of an ideal

We can get an upper bound for the terms in M by observing that each term M_i is

$$M_i = (n^i - n^{i-1}r_1 - \ldots - nr_{i-1} - r_i)(r_1 + \ldots + r_i)$$
$$< (n^i - r_1 - \ldots - r_{i-1} - r_i)(r_1 + \ldots + r_i) \leq (n^i/2)^2 :$$

each term is bounded above by $n^i/2$. So

$$M \leq (\frac{n}{2} + \frac{n^2}{2} + \ldots + \frac{n^{e-1}}{2}))^2 = \frac{n^2}{4}(\frac{n^{2e}-1}{n^2-1}).$$

An upper bound on the number of ideals

So the number $i(A)$ of ideals of A is a polynomial in p whose leading term is bounded above by

$$p^{\frac{n^2}{4}(\frac{n^{2e}-1}{n^2-1})}.$$

By comparison, the number $s(A)$ of subspaces of A is a polynomial in p whose highest degree term is

$$= p^{(\frac{n^2}{4})(\frac{n^e-1}{n-1})^2}.$$

So

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

where

$$t = (\frac{n^2}{4})(\frac{n^{2e}-1}{n^2-1} - \frac{(n^e-1)^2}{(n-1)^2}) \sim (\frac{n^2}{4})(-n^{2e}(n-1))$$

for large n or e.

An upper bound on the GCR

So, given the earlier result that the number of subgroups of $(A, \circ)$ is the same as the number of subgroups of $(A, +)$, we have:

Theorem

Let A be the $\mathbb{F}_p$-algebra $\mathbb{F}_p[x_1, x_2, \ldots x_n]$ with relations $A^{e+1} = 0$. Let L/K be a Galois extension with Galois group $G \cong (A, \circ)$ with a Hopf-Galois structure of type $N = (A, +)$. Then the Galois correspondence ratio

$$GCR(L/K, H) = (ideals\ of\ H)/(subgroups\ of\ G) \sim p^{-(\frac{n^2}{4})(n^{2e}(n-1))}$$

so is near 0 for large p, n or e.

The bi-skew brace case $e = 2$

For $e = 2$, $A^3 = 0$, so the algebra $A = \mathbb{F}_p[x_1, x_2]$ yields a bi-skew brace. In that case, the number of ideals of A is maximal when $r_1 = 0, r_2 = n^2/2$: the ideals with the maximal number of parameters are the subgroups of A^2. Then

$$\begin{aligned} i(A)/s(A) &\sim p^{(\frac{n^2}{2})^2 - (\frac{n+n^2}{2})^2} \\ &= \frac{1}{p^{\frac{2n^3+n^2}{2}}}. \end{aligned}$$

References

[Ch17] L. N. Childs, On the Galois correspondence for Hopf Galois structures, New York J. Math 23 (2017), 1-10.
[Ch18] L. N. Childs, Skew braces and the Galois correspondence for Hopf Galois structures, J. Algebra 511 (2018), 270-291.
[CG18] L. N. Childs, C. Greither, Bounds on the number of ideals in finite commutative nilpotent $\mathbb{F}_p$-algebras, arxiv:1706.02518; Publ. Math. Debrecen 92 (2018), 495-516.
[Ch19] L. N. Childs, Bi-skew braces and Hopf Galois structures, New York J. Math 25 (2019), 574-588.

References ctd.

[Omaha21] CGKKKTU, Hopf Algebras and Galois Module Theory, Math. Surveys and Monographs vol. 260, Amer. Math. Soc., 2021.
[Ch21] L. N. Childs, On the Galois correspondence for Hopf Galois structures arising from radical algebras and Zappa-Szep groups, Publ. Mat. (Barcelona) 65 (2021), 141-163.
[ST22] L. Stefanello, S. Trappeniers, On the connection between Hopf-Galois structures and skew braces, arXiv:2206.07610v2, 7 July 2022.
[ST22a] L. Stefanello, S. Trappeniers, On biskew braces and brace blocks, arXiv:2205.15073v3, 15 Dec. 2022.