J. D. H. Smith

Two enumeration principles for free algebras

Acta Universitatis Carolinae. Mathematica et Physica, Vol. 25 (1984), No. 1, 53--58

1984 ACTA UNIVERSITATIS CAROLINAE — MATHEMATICA ET PHYSICA VOL. 25. NO. 1

Two Enumeration Principles for Free Algebras

J. D. H. SMITH
Technische Hochschule Darmstadt*)

Received 30 March 1983

Two enumeration principles for finite free algebras in locally finite varieties, based respectively on essential dependence and linearity, are discussed and illustrated. A concept of linearly essential dependence of an algebraic operation on its arguments is then introduced, enabling these two principles to be combined. The technique obtained is applied to varieties of commutative Moufang loops. In particular, the free commutative Moufang loop of nilpotence class 4 and exponent 3 is shown to have cardinality $3^{d(n)}$, where

$$d(n) = n + \binom{n}{3} + 4\binom{n}{4} + 14\binom{n}{5} + 30\binom{n}{6} + 20\binom{n}{7}.$$

Jsou diskutovány a ilustrovány dva enumerační principy pro konečné algebry v lokálně konečných varietách, založené na podstatné závislosti a linearitě. Tato technika je aplikována na variety komutativních Moufangových lup.

Дискутируются и иллюстрируются два энумерационных принципа для конечных алгебр в локально конечых многообразиях, основанные на существенной зависимости и линеарности. Эта техника применяется к многообразиям коммутативных луп Муфанг.

1. Introduction

Let **T** be a locally finite variety of algebras, i.e. such that the free **T**-algebra on a finite set is itself finite. One then has the problem of specifying, for each natural number n, the cardinality of the free **T**-algebra on n generators. Notorious examples of this problem are furnished by distributive lattices ([1, p. 97]; [5]) and commutative Moufang loops ([8, Vopros 10.3]; [9, Problem 10.2]; [16]). The problem gains additional interest when its solution entails a detailed analysis of the structure of the free algebras. The current note looks at two principles that are useful in tackling the problem, illustrating their application with a number of examples. The principles themselves, examined in sections 2 and 3 respectively, are quite elementary, but combining them, as in the last section, enables one to simplify certain apparently complicated enumeration problems — such as those for exponent 3 commutative Moufang loops of nilpotence class 4 and 5.

*) Technische Hochschule Darmstadt FB4 AG1 Schlossgartenstrasse 7, D-6100 Darmstadt, West Germany.

2. Essential dependence

An n-ary operation $(x_1, \ldots, x_n)\, p$ of $\mathbf{T}$ is said to be *essentially dependent on* $\{x_1, \ldots, x_n\}$, *essentially n-ary*, or just *essential* (if specific reference to the arguments or arity is unnecessary), provided the element $(x_1, \ldots, x_n)\, p$ of the free $\mathbf{T}$-algebra XF on the set $X = \{x_1, \ldots, x_n\}$ does not lie in any subalgebra of XF generated by a proper subset of X (cf. [11, p. 37]). For example, in the variety of distributive lattices the operation $x \cup y$ is essentially binary, whereas $(x \cup y) \cap x$ is not.The first of the enumeration principles presupposes that it is easier to count the essentially n-ary operations rather than all of the n-aries. Let XF' denote the set of essentially n-ary elements of XF. Then (cf. [10, p. 181])

$$|XF| = \sum_{Y \subseteq X} |YF'|, \tag{2.1}$$

so that

it suffices to know each $|XF'|$ in order to determine each $|XF|$.

The relationship between the two is best expressed in terms of exponential generating functions [13, p. 97]. For each natural number n, let $\boldsymbol{n}$ be an n-element set. Define

$$f(x) = \sum_{n=0}^{\infty} |\boldsymbol{n}F| \frac{x^n}{n!}, \tag{2.2}$$

the exponential generating function for the cardinalities of the finite free algebras. Define

$$g(x) = \sum_{n=0}^{\infty} |\boldsymbol{n}F'| \frac{x^n}{n!}, \tag{2.3}$$

the generating function for the essential operations. These definitions may be interpred formally, or analytically if convergence obtains. (The formal interpretation is more generally applicable, but the analytic interpretation leads on to such refinements as asymptotic expansions.) Now by (2.1),

$$|\boldsymbol{n}F| = \sum_{r=0}^{n} \binom{n}{r} |\boldsymbol{r}F'|. \tag{2.4}$$

Thus

$$e^x g(x) = \left(\sum_{m=0}^{\infty} \frac{x^m}{m!}\right) \cdot \left(\sum_{r=0}^{\infty} |\boldsymbol{n}F'| \frac{x^r}{r!}\right) = \tag{2.5}$$

$$= \sum_{n=0}^{\infty} x^n \sum_{r+m=n} |\boldsymbol{r}F'| \cdot \frac{1}{r!} \cdot \frac{1}{m!} = \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{r=0}^{n} \binom{n}{r} |\boldsymbol{r}F'|, \quad \text{i.e.} \quad f(x) = e^x g(x).$$

An example of the use of (2.5), consider the variety $\mathbf{T}$ of normal bands [6, IV.5], i.e. idempotent ($aa = a$) entropic ($ab \,.\, cd = ac \,.\, bd$) semigroups ($ab \,.\, c =$

$= a \, . \, bc$). The normal band words essentially dependent on a set $X = \{x_1, \ldots, x_n\}$ of arguments may be written as $y_1 \ldots y_r$, where $\{x_1, \ldots, x_n\} = \{y_1, \ldots, y_r\}$. The value of such a word depends only on the choice of y_1 and y_r; there are n^2 such choices. Thus $|XF'| = n^2$ and $g(x) = \sum n^2 x^n/n! = (x + x^2) e^x$, whence by (2.5) $f(x) = (x + x^2) e^{2x}$, i.e. $|XF| = 2^{n-2} n(n+1)$ [6, Ex. IV.14]. A slightly more illuminating example is that of rectangular bands [6, Prop. IV.3.2], semigroups satisfying $aa = a$ and $abc = ac$. Here the only essential operations are x_1, x_1x_2, and x_2x_1. Thus $g(x) = x + x^2$ and $f(x) = (x + x^2) e^x$. The most trivial example is that of sets or right zero bands ($ab = b$), where $g(x) = x$ and $f(x) = xe^x$. The only essential operation is the identity mapping.

Elementary examples where the essentials are harder to count than the general operations are the varieties of vector spaces over a finite field $GF(q)$, where $|\boldsymbol{n}F| = q^n$ and $f(x) = e^{qx}$. In such cases (2.5) can then be regarded as a quick way of counting the essentials.

3. Use of linearity

In many locally finite varieties **T** the cardinality of the finite free algebras grows so fast that the series (2.2) and (2.3) diverge. For example, if **T** is the variety of bands (idempotent semigroups), $|\boldsymbol{n}F'| = \prod_{r=1}^{n-1} (n - r + 1)^{2^r}$ [6, IV(4.8)], or if **T** is the variety of groups of exponent 3, $|\boldsymbol{n}F| = 3^{\mathrm{d}(n)}$ with $\mathrm{d}(n) = n + \binom{n}{2} + \binom{n}{3}$ [7, Satz 1]. In the latter case $\mathrm{d}(n)$ seems to be the number to be looking at, not $|\boldsymbol{n}F|$. Now $\mathrm{d}(n)$ is the dimension of the vector space over $GF(3)$ obtained from the nilpotent group $\boldsymbol{n}F$ by taking the direct sum of the successive quotients down the lower central series. These quotients are certainly abelian groups, and become $GF(3)$-spaces on defining $x \mapsto x^{-1}$ to be scalar multiplication by -1. A general version of this situation leads to the second enumeration principle, the use of linearity.

From now on, consider $F : \mathrm{Set} \to \mathbf{T}$ as the free algebra functor from the category of sets to the category **T** of **T**-algebras and homomorphisms.

Hypothesis 3.1. Suppose given a variety **V** of vector spaces over a finite field ($GF(3)$ in the motivating example). Suppose given a functor $E : \mathbf{T} \to \mathbf{V}$ (the vector space construction in the example) preserving the cardinalities of underlying sets of finite algebras, and such that $A \subset B \in \mathbf{T}$ implies $AE \subset BE \in \mathbf{V}$.

Then the second enumeration principle is that for finite sets X,

it suffices to know each $\dim XFE$ *in order to determine each* $|XF|$.

Using this principle, the enumeration problem for **T** reduces to specification of the dimension $d(n) = \dim(\boldsymbol{n}FE)$ for each natural number n.

4. Linearly essential dependence

For the variety **T** if groups of exponent 3, as in the previous section, the use of linearity leads to the exponential generating function

$$f(x) = \sum_{n=0}^{\infty} d(n) \frac{x^n}{n!} \tag{4.1}$$

for $d(n)$, which is $(x + x^2/2! + x^3/3!) \, . \, e^x$. One is then tempted to ask what is counted by the corresponding $g(x)$ given by (2.5), namely $x + x^2/2! + x^3/3!$. To answer this question, consider the following

Definition 4.2. Under Hypothesis 3.3, **T**-operations having a set X of arguments exhibit *linearly essential dependence on their arguments* if they do not lie in the subspace of XFE spanned by the YFE as Y ranges over all proper subsets of X. The **T**-operations $(x_1, \ldots, x_n)\, p$ that have linearly essential dependence on their arguments $\{x_1, \ldots, x_n\}$ are also called *linearly essentially n-ary* or just *linearly essential*. Otherwise, $(x_1, \ldots, x_n)\, p$ is called *linearly inessential*.

In the motivating Burnside group example, the ternary operation $[x_1, x_2] \, . \, . \, [x_2, x_3]$ is linearly inessential, although it is essential.

Let $e(X)$ denote the codimension of the subspace of XFE consisting of linearly inessential operations with X as their set of arguments. Then in analogy with (2.1) one has

$$\dim XFE = \sum_{Y \subseteq X} e(Y)\,, \tag{4.3}$$

while (2.4) corresponds to

$$d(n) = \sum_{r=0}^{n} \binom{n}{r} e(r)\,. \tag{4.4}$$

Thus $g(x) = e^{-x} f(x)$ is the exponential generating function

$$g(x) = \sum_{n=0}^{\infty} e(n) \frac{x^n}{n!} \tag{4.5}$$

for the codimensions of the spaces of linearly inessential operations. For the variety of groups of exponent 3, the function $g(x) = x + x^2/2! + x^3/3!$ enumerates the bases $\{x_1\}$, $\{[x_1, x_2]\}$, and $\{[x_1, x_2, x_3]\}$ of complements of the spaces of linearly inessentials.

The technique just outlined is admirably suited to varieties **T** of commutative Moufang loops of exponent 3, which behave much like the variety of groups of exponent 3. In particular, such varieties are locally finite [4, Theorem VIII.11.3] and locally nilpotent [4, Theorem VIII.10.1], so there is a functor $E : \mathbf{T} \to \mathbf{V}$ defined exactly as for the Burnside groups. Let $\mathbf{N}_c(\mathbf{CML}_3)$ denote the variety of commutative Moufang loops of nilpotence class at most c. In the simplest non-trivial case, namely

$c = 2$, $\{x_1\}$ and $\{(x_1, x_2, x_3)\}$ may be chosen as bases of complements of the spaces of linearly inessentials, so

$$g(x) = x + \frac{x^3}{3!} \tag{4.6}$$

and $f(x) = (x + x^3/3!) \,.\, e^x = \sum_{n=1}^{\infty} \left(n + \binom{n}{3}\right) x^n/n!$. One thus recovers Bruck's formula [3, Theorem 9A(v)]

$$d(n) = n + \binom{n}{3}. \tag{4.7}$$

For $\mathbf{N}_3(\mathbf{CML}_3)$, one has (by [4, VIII] and [15]) $\{x_1\}$, $\{(x_1, x_2, x_3)\}$, $\{(x_{1\pi}, x_{2\pi}, x_{3\pi}; x_{4\pi}) \mid \pi \in \langle(1234)\rangle\}$, and $\{(x_{1\pi}, x_{2\pi}, x_{3\pi}! \, x_{4\pi}, x_{5\pi}) \mid \pi \in \langle(12345)\rangle - \{(1)\}\}$ as bases of complements to the linearly inessentials. Thus in this case

$$g(x) = x + \frac{x^3}{3!} + 4\frac{x^4}{4!} + 4\frac{x^5}{5!} \tag{4.8}$$

and

$$f(x) = \left(x + \frac{x^3}{3!} + 4\frac{x^4}{4!} + 4\frac{x^5}{5!}\right). e^x = \sum_{n=1}^{\infty} \left(n + \binom{n}{3} + 4\binom{n}{4} + 4\binom{n}{5}\right)\frac{x^n}{n!},$$

whence the well-known formula

$$d(n) = n + \binom{n}{3} + 4\binom{n+1}{5} \tag{4.9}$$

(cf. [2, Prop. 4.5.6], [12, p. 68], [14]).

For $\mathbf{N}_4(\mathbf{CML}_3)$, $g(x)$ takes the form

$$g(x) = x + \frac{x^3}{3!} + 4\frac{x^4}{4!} + 4\frac{x^5}{5!} + 10\frac{x^5}{5!} + 30\frac{x^6}{6!} + 20\frac{x^7}{7!}. \tag{4.10}$$

The fifth term here corresponds to associators of shape (2) [15, §2], the sixth to shape (1, 0), and the seventh to shape (0, 0, 0) (cf. [16, §8]). Then

$$d(n) = n + \binom{n}{3} + 4\binom{n}{4} + 14\binom{n}{5} + 30\binom{n}{6} + 20\binom{n}{7}. \tag{4.11}$$

References

[1] Balbes R. and Dwinger P.: Distributive Lattices, University of Missouri Press, Columbia Missouri 1974.

[2] Beneteau L.: Free commutative Moufang loops and anticommutative graded rings, J. Alg. 67 (1980), 1–35.

[3] BRUCK R. H.: Contributions to the theory of loops, Trans. Amer. Math. Soc. 60 (1946), 245—354.
[4] BRUCK R. H.: A Survey of Binary Systems, Springer, Berlin 1958.
[5] DEDEKIND R.: Über Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler, Ges. Werke Bd. 2, 103—148.
[6] HOWIE J. M.: An Introduction to Semigroup Theory, Academic Press, London 1976.
[7] LEVI F. and van der WAERDEN B. L.: Über eine besondere Klasse von Gruppen, Abh. Math. Sem. Hamburg 9 (1933), 154—158.
[8] MANIN JU. I.: Kubičeskie Formy, Nauka, Moskva 1972.
[9] MANIN JU. I. (tr. HAZEWINKEL M.): Cubic Forms, North-Holland, Amsterdam 1974.
[10] MARCZEWSKI E.: Independence in abstract algebras, Colloq. Math. 14 (1966), 169—188.
[11] PÖSCHEL R. and KALUŽNIN L. A.: Funktionen- und Relationenalgebren, Deutscher Verlag der Wissenschaften, Berlin 1979.
[12] RAY-CHAUDHURI D. K.: Affine triple systems, in Combinatorics and Graph Theory (ed. S. B. Rao), Springer Lecture Notes in Mathematics 885, Berlin 1981.
[13] ROTA G.-C.: Finite Operator Calculus, Academic Press, New York 1975.
[14] ROTH R.: Hall triple systems and commutative Moufang exponent three loops, Ph. D. dissertation 1979, Ohio State University.
[15] SMITH J. D. H.: A second grammar of associators, Math. Proc. Camb. Phil. Soc. 84 (1978), 405—415.
[16] SMITH J. D. H.: Commutative Moufang loops and Bessel functions, Inv. Math. 67 (1982), 173—187.