Discrete Mathematics 118 (1993) 197–206
North-Holland

The equations $D^k Y = X^n$ in combinatorial species

Dayanand S. Rajan*

Department of Computer and Information Sciences, University of Delaware, Newark, DE 19713, USA

Received 8 August 1990

Abstract

Rajan, D.S., The equations $D^k Y = X^n$ in combinatorial species, Discrete Mathematics 118 (1993) 197–206.

The category of *combinatorial species* was introduced by Joyal, and has been studied extensively by him and others. This category is equipped with a derivative operation (endofunctor). This allows one to differentiate species in a manner similar to differentiating power series. We solve, completely, the family of differential equations $D^k y = X^n$ for species. For this, we use results on the conjugacy classes of sharply k-transitive groups. We provide, also, a new proof of a sharpened version of Zassenhaus' theorem on sharply 2-transitive groups of type I.

1. Introduction

The category of *combinatorial species*, which we call *Species*, was introduced by Joyal in [2], and has been studied extensively by him and others [3, 4, 7, 8]. *Species* is a category rich in structure, as we will indicate in this section. One of the important endofunctors on *Species* is the derivative. Several people [2–4, 7, 8] have studied this endofunctor, and some [2, 3] have solved several classes of differential equations in species. In this paper, we find nonisomorphic solutions to the family of differential equations $D^k y = X^n$, $k \geqslant 0$. By Corollary 1.4, this is equivalent to finding the conjugacy classes of sharply k-transitive groups for $k \geqslant 1$. For the cases $k > 2$ these are known and, in Section 2, we quote results from permutation group theory and interpret them for our purposes. For the case $k = 2$, we do more: Zassenhaus' construction (cf. [1, Ch. XII, Section 9]) of all possible sharply 2-transitive groups does not immediately tell us when two of the constructed groups are conjugate to each other. In Section 3, we provide a new, less computational, proof of Zassenhaus' construction and describe

Correspondence to: Dayanand S. Rajan, Department of Computer and Information Sciences, University of Delaware, Newark, DE 19713, USA.

* This work was part of the author's doctoral dissertation, completed under the guidance of Prof. S.H. Schanuel at the State University of New York at Buffalo, USA.

the set of conjugacy classes of sharply 2-transitive groups. Section 4 is a summary of our results.

Let *Set* be the category of sets. Let $\boldsymbol{B}$ denote the category of finite sets and bijections between finite sets. Let *Species* denote the catgory $Set^{\boldsymbol{B}}$ of all functors $\boldsymbol{B} \to Set$ and natural transformations between them. If E is an object of $\boldsymbol{B}$ and A is a species, $A(E)$ is a set whose elements are called *A-structures* (on E). A *map of species* f between species A and B is a natural transformation between A and B. A species A *is finitary* if, for each E in $\boldsymbol{B}$, the cardinality of $A(E)$ is finite. A finitary species A is *finite* if there is an n for which $A(E)$ is empty for all E in $\boldsymbol{B}$ with cardinality at least n.

Let $\underline{n}$ denote the set $\{0, \ldots, n-1\}$. The species X^n is the representable functor $\boldsymbol{B}(\underline{n}, -)$. We denote the species X^0 by 1. Let $\underline{n}!$ denote the group, under composition, of all permutations of $\underline{n}$. Let H be a subgroup of $\underline{n}!$. Then the species X^n/H is defined by $(X^n/H)(E) = \boldsymbol{B}(\underline{n}, E)/\sim$, where, for any bijection $f: \underline{n} \to E$, $f \sim f \circ h$ for all $h \in H$.

The sum of two species is their coproduct. A species is a *molecule* if it is not the 0 species and cannot be decomposed as the sum of two nonzero species. Let M be a molecule. The unique n for which $M(\underline{n}) \neq \phi$ is called the *degree* of M. We say that a species *has degree n* if it is the nonempty sum of molecules all of degree n. A *constant species* is a species of degree 0. M_n, $n \geqslant 0$, denotes the set of isomorphism classes of molecules of degree n.

Every isomorphism class of species A can be written as a sum of species of distinct degree: $A = \sum_{n \geqslant 0} A_n$, where A_n is a species of degree n. If A is finitary, we can represent A_n as a finite sum of molecules from M_n. The following proposition aids us by giving a criterion for two molecules to be isomorphic.

Proposition 1.1. (i) *Every molecule is isomorphic to* X^n/H *for some* $H \leqslant \underline{n}!$.

(ii) *Two molecules* X^n/H *and* X^m/K *are isomorphic iff* $n = m$ *and* H *and* K *are conjugate in* $\underline{n}!$.

The *derivative* functor $D: Species \to Species$ is defined as follows: For a species A and an object E of $\boldsymbol{B}$, $(DA)(E) = A(E+1)$.

If an isomorphism class of finitary species is represented by its molecular decomposition, we can calculate its derivative, term by term, just as for power series. The following proposition gives an expression for the derivative of a molecule.

Proposition 1.2 (cf. Yeh [8]). *Let* $H \leqslant \underline{n}!$ *and let* $O(n, H)$ *be a complete set of representatives for the orbits in* $\underline{n}$ *under the action of* H. *For* i *in* $\underline{n}$, *let* H_i *be the stabilizer of* i, *that is,* H_i *is the subgroup of* $\underline{n}!$ *of those permutations* h *with* $h(i) = i$. *The derivative of the molecule* X^n/H *is isomorphic to the species* $\sum_{i \in O(n, H)} X^{n-1}/H_i$.

Species is equipped with a tensor product (cf. [2]) and the derivative functor satisfies Leibniz' rule with respect to this tensor product: For species A and B, $D(A \otimes B) \cong (DA) \otimes B + A \otimes (DB)$. Also, the derivative of X^n is isomorphic to nX^{n-1}

(the n-fold coproduct). The behaviors of species and power series with respect to the derivative operation are very similar.

The solutions in species to some differential equations can be calculated fairly easily. For example, we can easily show that there are exactly two solutions to the differential equation $DY = Y$. One is $\exp(X)$ which satisfies the boundary condition $Y(0) = 1$ and the other is $\sum_{n \geqslant 0} X^n / A_n$, A_n being the alternating group of degree n, which satisfies the boundary condition $Y(0) = 2$. Joyal [2] and Labelle [3] have studied more complicated differential equations for species. It is usually not easy (nor desirable) to describe solutions of most of these differential equations of species in terms of molecular species. In our case, we can, and will, do so.

We have the advantage that most of the facts we need for such an explicit description are important theorems in permutation group theory. For the cases $k > 2$, we will directly apply these theorems and provide explicit references to them. For the case $k = 2$, we will obtain and sharpen Zassenhaus' result using a less computational proof.

In view of the following lemma, we will consider, from the next section onwards, only molecular solutions of $D^k Y = X^n$, and by 'solution' we will mean a molecular solution.

Lemma 1.3. *A molecule A is a solution of the equation $D^k Y = X^n / H$ iff $A \cong X^{n+k}/G$, where G is k-transitive, of degree $n+k$, $H \leqslant G$, and the stabilizer in G of some (and hence every) set of k distinct elements is conjugate to H in G. Moreover, for every species P which is a sum of molecules of degree less than k, $A + P$ is also a solution.*

Corollary 1.4. *X^{n+k}/G is a solution to the equation $D^k Y = X^n$ iff G is a sharply k-transitive group of degree $n+k$.*

2. The cases $k > 2$

There are very few groups that are k-transitive for $k \geqslant 4$, and even fewer that are sharply k-transitive.

Theorem 2.1 (Jordan) (cf. [1, Ch. XII, pp. 325–327]). (i) *The sharply 4-transitive groups are $\underline{4}!$, $\underline{5}!$, the alternating group A_6 and the Mathieu group of degree 11, M_{11}.*

(ii) *The sharply 5-transitive groups are $\underline{5}!$, $\underline{6}!$, the alternating group A_7 and the Mathieu group of degree 12, M_{12}.*

(iii) *If $k \geqslant 6$, the sharply k-transitive groups are $\underline{k}!$, $\underline{(k+1)}!$ and A_{k+2}.*

Corollary 2.2. *If $k \geqslant 4$, the species $X^k/\underline{k}!$, $X^{k+1}/\underline{(k+1)}!$, and X^{k+2}/A_{k+2} are solutions to the equation $D^k Y = X^n$ for $n = 0, 1, 2$, respectively. These are the only (molecular) solutions except in the cases $D^4 Y = X^7$ and $D^5 Y = X^7$ which have solutions X^{11}/M_{11} and X^{12}/M_{12}, respectively.*

The solutions when $k=3$ and $k=2$ are given in terms of transformations on finite fields. We recall a few definitions.

Definition 2.3. Let F denote a finite field of order p^f, F^* the multiplicative group of F, and $(F^*)^n$ the subgroup of F^* consisting of n-th powers of elements of F^*. $\mathrm{Aut}(F)$ denotes the group of field automorphisms of F and $F!$ denotes the group of all permutations of the underlying set of F.

Definition 2.4. Let $\mathrm{GL}(2, p^f)$ be the group of 2×2 invertible matrices over F. Let $P=(F^2\setminus\{0\})/F^*$. Then $\mathrm{PGL}(2, p^f)=\mathrm{GL}(2, p^f)/F^*$ is the projective linear group whose action on P is the one induced by the action of $\mathrm{GL}(2, p^f)$.

If $f=2m$ and $p>2$, let α be the unique field automorphism (of F) of order 2. Then α acts on the elements of P, coordinatewise. $M(p^f)$ is the subgroup of $\mathrm{PGL}(2, p^f)\langle\alpha\rangle$ generated by the set of all elements of the form $M\circ\alpha$, where $M\in\mathrm{PGL}(2, p^f)$ and $\det(M)$ is not a square in F.

$M(p^f)$ consists exactly of transformations of the following two forms:

(i) $(ax+b)/(cx+d)$, with a, b, c, d in F, $ad-bc$ a square in F,

(ii) $(a\alpha(x)+b)/(c\alpha(x)+d)$, with a, b, c, d in F, $ad-bc$ not a square in F.

Theorem 2.5 (Zassenhaus) (cf. [1, Ch. XI, pp. 173 and 176]). *If G is a sharply 3-transitive group, then G has degree p^f+1 for some prime p and $f\in N$. G is similar to $\mathrm{PGL}(2, p^f)$ or if f is even and $p>2$, then G could be similar instead to $M(p^f)$.*

Corollary 2.6. *The equation $D^3y=X^n$ has solutions iff $n=p^f-2$ for some prime p and $f\in N$. $X^{n+3}/PGL(2, p^f)$ is then a solution. The only other solution, $X^{n+3}/M(p^f)$, occurs iff $p>2$ and f is even.*

3. The case $k=2$

Definition 3.1. Let $F^*\propto\mathrm{Auf}(F)$ denote the semi-direct product of F^* with the group of automorphisms $\mathrm{Aut}(F)$. That is, $F^*\propto\mathrm{Aut}(F)$ is the group consisting of all pairs (c, α), where $c\in F^*$ and $\alpha\in\mathrm{Aut}(F)$, with the group multiplication defined by

$$(c, \alpha)\circ(d, \beta)=(c\alpha(d), \alpha\circ\beta).$$

There is a canonical exact sequence

$$1\to F^*\xrightarrow{\iota} F^*\propto\mathrm{Aut}(F)\xrightarrow{\pi}\mathrm{Aut}(F)\to 1,$$

where $\iota(F^*)$ is the set of all pairs (c, id), $c\in F^*$, a normal subgroup, which we identify with F^*. For (c, α) in $F^*\propto\mathrm{Aut}(F)$, the transformation $x\mapsto c\alpha(x)$, x in F, is called a semi-linear transformation on F.

Theorem 3.2 (Zassenhaus) (cf. [1, Ch. XII, Section 9], [6, p. 259]). *Let G be a sharply 2-transitive permutation group acting on a set E. Then we can identify the elements of E with the underlying set of a finite field F of order p^f, for some prime p and natural number $f>0$, so that $G=TS$, where T is the set of translations of F, and $S=G_0$ is either a subgroup of $F^* \propto \mathrm{Aut}(F)$ (we then say that S is of type I) or S is one of the seven groups listed in the appendix.*

In order to find the set of nonisomorphic solutions to $D^2Y=X^n$, we have to determine the set of conjugacy classes of sharply 2-transitive groups of degree n, and we will proceed in that direction.

Let G and G' be sharply 2-transitive groups of degree p^f. Since any two finite fields of the same degree are isomorphic, we can, by composing with such an isomorphism, assume that G and G' are represented as TS and TS' with respect to the finite field F. Then they are conjugate in $F!$ if and only if S and S' are conjugate to each other. For groups S, not of type I, isomorphism implies conjugacy. For groups of type I, this is not the case, as we will see.

If S is of type I, the canonical projection π from $F^* \propto \mathrm{Aut}(F)$ onto $\mathrm{Aut}(F)$ maps S onto a subgroup of order n for some n dividing f. Let $q^n=p^f$.

Definition 3.3. Define S_n and R_n by

$$S_n=\{S \leqslant F^* \propto \mathrm{Aut}(F) \mid |S|=|F^*|,\ S \cap F^* = (F^*)^n,\ n \text{ the least such}\}$$

and

$$R_n=\{S \in S_n \mid S_n \text{ is transitive on } F^*\}.$$

Then the elements of R_n are exactly the groups of type I.

Proposition 3.4. *Let Q_n be the subgroup of $\mathrm{Aut}(F)$ of order n. Then the following are equivalent:*

(i) $S \in S_n$,

(ii) $|S|=|F^*|$ *and* $\pi(S)=Q_n$,

(iii) $1 \to (F^*)^n \xrightarrow{i} S \xrightarrow{\pi} Q_n \to 1$ *is exact.*

Proof. This follows directly from the fact that $\mathrm{Ker}\,\pi$ has order $|F^*|/n$ and F^* is cyclic. □

Definition 3.5. Let G be a group equipped with a homomorphism into the group of automorphisms of an abelian group A (so A is a left G-module). Denote the action of an element g of G on an element of A by $g \cdot a$. A *derivation* from G to A is a function $D: G \to A$ so that, for every $g, h \in G$, $D(gh)=g \cdot D(h)+D(g)$. A derivation is also called a 'crossed homomorphism'. It will be convenient sometimes, as in our case, to use multiplicative notation instead of the additive one. $\mathrm{Der}(G, A)$ denotes the set of all derivations from G to A (for a fixed action).

Lemma 3.6. *There is a bijection between* $\mathrm{Der}(Q_n, F^*/(F^*)^n)$ *and* S_n.

Proof. Let π_1 be the canonical projection $F^* \to F^*/(F^*)^n$. Given $S \in S_n$, let $\mathrm{ev}_S : S \to F^*$ be the function 'evaluate at 1'. Note that for subgroups S and S' in S_n, $\mathrm{ev}_S = \mathrm{ev}_{S'}$ iff $S = S'$. Define $D = \varphi(S) : Q_n \to F^*/(F^*)^n$ by $D \circ \pi = \pi_1 \circ \mathrm{ev}_S$. We now have the following diagram:

$$\begin{array}{ccccccccc} 1 & \to & (F^*)^n & \xrightarrow{i} & S & \xrightarrow{\pi} & Q_n & \to & 1 \\ & & \| & & \downarrow \mathrm{ev}_S & & \downarrow D=\varphi(S) & & \\ 1 & \to & (F^*)^n & \xrightarrow{i} & F^* & \xrightarrow{\pi_1} & F^*/(F^*)^n & \to & 1 \end{array}$$

D is then a derivation.

Since π is a surjective homomorphism, we need only to show that for $s, t \in S$,

$$D \circ \pi(s \circ t) = \pi(s)(D \circ \pi(t)) \cdot D \circ \pi(s).$$

Let $s = (c, \alpha)$ and let $t = (d, \beta)$. Then

$$D \circ \pi(s \circ t) = \pi_1 \circ \mathrm{ev}_S(c\alpha(d), \alpha \circ \beta) = \pi_1(c\alpha(d)) = \pi_1(c) \cdot \pi_1(\alpha(d))$$

$$= \pi_1 \circ \mathrm{ev}_S(c, \alpha) \cdot \alpha(\pi_1 \circ \mathrm{ev}_S(d, \beta)) = (D \circ \pi(s)) \cdot (\pi(s)(D \circ \pi(t))).$$

So we get a map $\varphi : S_n \to \mathrm{Der}(Q_n, F^*/(F^*)^n)$.

Conversely, given D, define $S = \psi(D)$ by

$$S = \{(a, \sigma) \in F^* \propto \mathrm{Aut}(F) \mid \pi_1(a) = D(\sigma)\}.$$

(S is the pullback in $F^* \propto \mathrm{Aut}(F)$ of π_1 and D.) We have to show that S is a group. For $(c, \alpha), (d, \beta) \in S$, $(c, \alpha) \circ (d, \beta) = (c\alpha(d), \alpha \circ \beta) \cdot D(\alpha \circ \beta) = \alpha(D(\beta)) \cdot (D(\alpha)) = \pi_1(c) \cdot \alpha(\pi_1(d)) = \pi_1(c) \cdot \pi_1(\alpha(d)) = \pi_1(c\alpha(d))$. This gives us a map $\psi : \mathrm{Der}(Q_n, F^*/(F^*)^n) \to S_n$.

$(a, \sigma) \in \psi(\varphi(S))$ iff $\varphi(S)(\sigma) = \pi_1(a)$ iff $(a, \sigma) \in S$. So both the composites $\psi \circ \varphi$ an $\phi \circ \psi$ are the identity. □

Lemma 3.7. *Let the notation be as in Lemma* 3.6, *and let* σ *generate* Q_n. *Then the map defined by* $S \mapsto \varphi(S)(\sigma)$ *is a bijection between* S_n *and the set of those elements of* $F^*/(F^*)^n$ *whose order divides* $(q^n - 1)/(q - 1)$.

Proof. Since Q_n is cyclic, and

$$\varphi(S)(\sigma^i) = \sigma^{i-1}(\varphi(S)(\sigma)) \cdots \varphi(S)(\sigma) = (\varphi(S)(\sigma))^{(q^i - 1)/(q-1)}$$

for $1 \leqslant i \leqslant n$, $\varphi(S)$ is determined by $\varphi(S)(\sigma)$. Also, $\varphi(S)(\mathrm{id}) = 1$, so the order of $\varphi(S)(\sigma)$ divides the order of $F^*/(F^*)^n$. □

Proposition 3.8. *With notation as in Lemma* 3.6, φ *induces a bijection from* R_n *to the set of all bijections in* $\mathrm{Der}(Q_n, F^*/(F^*)^n)$. *Also, if* $R_n \neq \phi$ *then* n *divides* $(q^n - 1)/(q - 1)$.

Proof. Let S be in R_n. Then ev_S is a bijection because S is transitive. So $\varphi(S)$ is surjective and since $|Q_n| = |F^*/(F^*)^n| < \infty$, $\varphi(S)$ is bijective.

Conversely, if D is a bijection and $s, t \in S = \varphi^{-1}(D)$, $\mathrm{ev}_S(s) = \mathrm{ev}_S(t) \Rightarrow \pi_1 \circ \mathrm{ev}_S(s) = \pi_1 \circ \mathrm{ev}_S(t) \Rightarrow D \circ \pi(s) = D \circ \pi(t) \Rightarrow \pi(s) = \pi(t)$. So, $s = \mathrm{ev}_S(s)\pi(s) = \mathrm{ev}_S(t)\pi(t) = t$. □

Corollary 3.9. *φ is a bijection from R_n to the set of generators b of $F^*/(F^*)^n$ for which if $1 \leqslant i \leqslant n$, $b^{(q^i-1)/(q-1)} = 1$ iff $i = n$.*

Proof. If $\varphi(S)$ is a bijection and $1 \leqslant i \neq j \leqslant n$, $\varphi(S)(\sigma^i) \neq D(\sigma^j)$. So $\varphi(S)(\sigma)$ is a generator for $F^*/(F^*)^n$. □

Such generators exist iff n divides $(q^n-1)/(q-1)$ but n does not divide $(q^i-1)/(q-1)$ for $1 \leqslant i < n$. This is Zassenhaus' condition on (q, n).

What remains to be found, now, is the set of nonconjugate representations TS, with T constant and S varying. We quote a theorem from the literature (cf. [6, Proposition 19.8, p. 244]) which makes our proof easy.

Theorem 3.10. *Let G be a group that acts faithfully and additively on a vector space V of order p^f over $\mathrm{GF}(p)$. Let G contain a normal cyclic subgroup N, which acts irreducibly on V. Then we can identify V with the additive group F in such a way that $G \leqslant F^* \propto \mathrm{Aut}(F)$. Moreover, a permutation $g \in G$ commutes with every element of N (that is, g is in the centralizer of N in G) iff g is in $F^* \cap G$.*

In the theorem below, we will be applying this result to a group acting on the vector space T of all translations of F.

Lemma 3.11. *Let T be the group of all translations of F and let TS be the sharply 2-transitive group with S of type I. If $S = NQ_n$ in the above notation, then N acts irreducibly, by conjugation, on the vector space T (over $GF(p)$).*

Proof. If $n = 1$, then $N = F^*$ and so the result is obvious. Suppose $n > 1$ and let $0 \neq T_1$ be an N-invariant subspace of T. Let $t_a \in T_1$. Then if $x \in F_N$ the subfield of F generated by $(F^*)^n$, $t_{xa} \in T_1$. We will show that $F_N = F$, so that $T_1 = T$.

Suppose not. Then let $|F_N| = p^d$, $d \leqslant f/2$. Then

$$|(F^*)^n| = \frac{p^f - 1}{n} = \frac{(p^{f/2}-1)(p^{f/2}+1)}{n} \geqslant (p^d - 1)\frac{(p^{f/2}+1)}{n}.$$

But $f \geqslant n \geqslant 2$ and $p \geqslant 2$, so $(p^{f/2}+1)/n > 1$, giving the contradiction that $|(F^*)^n| > F_N^*|$. □

Lemma 3.12. *Let $n < q$. Then $q^n - 1 \geqslant n^2(q-1)$ and equality holds iff either $n = 1$ or $n = 2$ and $q = 3$.*

Proof. If $n \geqslant 3$, $(q^n-1)/(q-1)=q^{n-1}+\cdots>n^2$ since $q>n$. If $n=2$ then $q+1=(q^2-1)/(q-1)\geqslant 4=n^2$, since $q>n$, and equality holds iff $q=3$. If $n=1$ the result is obvious. □

Theorem 3.13. *Let TS_1, TS_2 be sharply 2-transitive groups of degree p^f and with S_1 and S_2 in R_n. If TS_1 is conjugate to TS_2 via $\alpha \in F!$, then α is a semi-linear transformation.*

Proof. Conjugation by α maps T onto itself because T is the only subgroup of order p^f in each of TS_1 and TS_2, so fixes $t_0=\mathrm{id}_F$. S_1 and S_2 are the only subgroups of order p^f-1 of TS_1 and TS_2, respectively, that fix t_0 (under conjugation), so α must take S_1 to S_2.

Now, S_1, S_2 are both isomorphic to NQ_n in the notation above. N is normalized by α: Let $x=(c, \mathrm{id})$ be a generator for N. Then the conjugate x' of x by α has order $(q^n-1)/n$. If x' is not in N, then it has order dividing $n(q-1)$. This means that $q^n-1 \leqslant n^2(q-1)$, which by the preceding lemma happens only if either $n=1$ or $n=2$ and $q=3$. In both these cases, we can check by inspection that $TS_1=TS_2$. So N is always normalized by α.

Now, consider the group $N\langle\alpha\rangle$ generated by N and α, acting on the vector space T of translations by conjugation. N is a normal subgroup of this group that acts faithfully and irreducibly (by Lemma 3.12) on T (considered as a vector space over $GF(p)$). So, by the preceding theorem, $N\langle\alpha\rangle$, and in particular α is contained in $F^* \propto \mathrm{Aut}(F)$. □

Corollary 3.14. *Let (q, n), $q^n=p^f$, satisfy Zassenhaus' condition. Then there is a bijection between the set of conjugacy classes of groups S in R_n, and the set of costs of the subgroup generated by p in the multiplicative group of units in $\mathbf{Z}/\gcd(n, q-1)\mathbf{Z}$.*

Proof. Let $S \in R_n$ and let $\varphi(S)(\sigma)=b$. The orbit of b under the action, on S, of conjugation by elements of $F^* \propto \mathrm{Aut}(F)$, induces an action on the set $F^*/(F^*)^n$. Under this induced action, the orbit of b is the set $\{b^{p^i}a^{q-1}(F^*)^n \mid a \in F^*, i=0, 1, \ldots\}$. That is, S' is a conjugate of S if $\varphi(S')(\sigma)$ is of the form b^{p^i} modulo the group $(F^*)^{\gcd(n,(q-1))}$. The result now follows because b is in the group of units of $F^*/(F^*)^{\gcd(n,q-1)}$. □

Corollary 3.15. *There are isomorphic nonconjugate sharply 2-transitive groups.*

Proof. Let $p=3$ and $f=16$. Then if $n=8$ and $q=9$, (n, q) satisfies Zassenhaus' condition. There are two cosets of $\langle 3\rangle$ in the group of units in $\mathbf{Z}/8\mathbf{Z}$. So there are two isomorphic nonconjugate sharply 2-transitive groups of type I and degree 3^{16}. □

In the following corollary, we interpret our result in terms of species.

Corollary 3.16. (i) *The equation $D^2y=X^n$ has solutions iff $n=p^f-2$ for some prime p and natural number f. X^{n+2}/G is then a solution if G is a sharply 2-transitive group.*

(ii) *If $p^f \neq 5^2, 7^2, 11^2, 23^2, 29^2, 59^2$, then, for each pair (q, m) with $q^m = p^f$ and (q, m) satisfying Zassenhaus' condition, the set of isomorphism classes of solutions X^{p^f}/G is in bijection with the set of cosets of $\langle p \rangle$ in the multiplicative group of units of $\mathbf{Z}/\gcd(m, q-1)\mathbf{Z}$. G is similar to TS, where T is the group of all translations and S is a group in $S_m(I)$.*

(iii) *If p^f is one of $5^2, 7^2, 11^2, 23^2, 29^2, 59^2$, then there are exactly two nonisomorphic solutions, X^{p^f}/G. G is (similar to) TS, where T is the group of all translations and S is either the group of all nonzero scalar multiplications or is one of the seven groups listed in the appendix.*

4. Summary

(i) $Dy = X^n$ always has a solution. Every solution is of the form X^{n+1}/G, where G is a group of order (and degree) $n+1$. Since any group acts regularly on itself (by left multiplication) there is a bijection between the solutions to $Dy = X^n$ and the isomorphism classes of groups of order $n+1$.

(ii) $D^2 y = X^n$ has a solution iff $n = p^f - 2$ for some prime p and natural number f.

(iii) $D^3 y = X^n$ has a solution iff $n = p^f - 2$ for some prime p and natural number f. This does not mean that every solution to $D^2 y = X^n$ can be antidifferentiated. In fact, a solution X^{n+2}/G of $D^2 y = X^n$ can be antidifferentiated iff G is the affine group of $GF(p^f)$ or, if f is even, the group generated by the semilinear transformations $x \mapsto a\alpha(x) + b$ over $GF(p^f)$, where α is the automorphism of order 2.

(iv) $D^4 y = X^n$ and $D^5 y = X^n$ have solutions iff $n = 0, 1, 2, 7$.

(v) $D^k y = X^n$, $k \geqslant 6$ has solutions iff $n = 0, 1, 2$.

Let A and B be molecules with $D^k A \cong D^k B \cong X^n$ for some natural numbers k, n. If also $D^i A \cong D^i B$, for some $0 < i < k$, does it follow that $A \cong B$? The answer is no, for $k = 1$ and $k = 2$. $D^3 A \cong D^3 B \cong X^n$ and $DA \cong DB$, together, imply $A \cong B$, but $D^3 A \cong D^3 B \cong X^n$ and $D^2 A \cong D^2 B$, together, do not. For $k > 3$, $D^k A \cong D^k B \cong X^n$, by itself, implies $A \cong B$.

Appendix

Subgroups S of types II and III

In the sequel, $GL(n, q)$ represents the group of invertible $n \times n$ matrices with entries in $GF(q)$, the finite field with q elements. $SL(n, q)$ represents the subgroup of $GL(n, q)$ consisting of matrices whose determinant is 1.

Type II (Solvable but not of type I)

(1) $p^f = 5^2$, $S \sim SL(2, 3)$. S is generated by

$$\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & -2 \end{pmatrix}.$$

(2) $p^f = 7^2$, $S \sim GL(2,3)$. S is generated by

$$\begin{pmatrix} 2 & 3 \\ 3 & -2 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -2 \\ -3 & -1 \end{pmatrix}, \quad \begin{pmatrix} 3 & -1 \\ 3 & -3 \end{pmatrix}.$$

(3) $p^f = 11^2$, $S \sim SL(2,3) \times \boldsymbol{Z}/5\boldsymbol{Z}$. S is generated by

$$\begin{pmatrix} 1 & 3 \\ 3 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} -5 & 4 \\ 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

(4) $p^f = 23^2$, $S \sim GL(2,3) \times \boldsymbol{Z}/11\boldsymbol{Z}$. S is generated by

$$\begin{pmatrix} 3 & 6 \\ 6 & -3 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -4 \\ -5 & -2 \end{pmatrix}, \quad \begin{pmatrix} 4 & -6 \\ -1 & -4 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Type III (Not solvable)

(1) $p^f = 11^2$, $S \sim SL(2,5)$. S is generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}.$$

(2) $p^f = 29^2$, $S \sim SL(2,5) \times \mathbf{Z}/7\mathbf{Z}$. S is generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}, \quad \begin{pmatrix} -13 & 0 \\ 0 & -13 \end{pmatrix}.$$

(3) $p^f = 59^2$, $S \sim SL(2,5) \times \mathbf{Z}/29\mathbf{Z}$. S is generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}, \quad \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}.$$

References

[1] B. Huppert and N. Blackburn, Finite groups III, Grundlehren Math. Wiss. 243 (1982).
[2] A. Joyal, Une théorie combinatoire des séries formelles, Adv. Math. 42 (1981) 1–82.
[3] G. Labelle, On combinatorial differential equations, J. Math. Anal. Appl. 113 (1986) 344–381.
[4] G. Labelle, On the generalized iterates of Yeh's combinatorial K-species, J. Combin. Theory Ser. A 50 (1989) 235–258.
[5] S. MacLane, Categories for the working mathematician, Graduate Texts in Math. 5 (1971).
[6] D. Passman, Permutation groups, in: Math. Lecture Notes Series (Benjamin, New York, 1968).
[7] D.S. Rajan, Differentiation and integration of the combinatorial species of Joyal, Ph.D. Dissertation, State University of New York at Buffalo, New York, 1989.
[8] Y.N. Yeh, On the combinatorial species of Joyal, Ph.D. Dissertation, State University of New York at Buffalo, New York, 1985.