数理解析研究所講究録
第 794 巻 1992 年 18-29

Groups and Generating Functions

吉田知行 (Tomoyuki YOSHIDA 北大・理)

1. Generating Functions

Let $a_0, a_1, \cdots, a_n, \cdots$ be a sequence of numbers. Then the (ordinary) generating function associated with this sequence is defined by

$$A(x) := \sum_{n=0}^{\infty} a_n x^n.$$

Example: Fibonacci numbers $F_0, F_1, \cdots$ have the following well-known recurrence formula:

$$F_0 = F_1 = 1, \quad F_n + 1 = F_n + F_{n-1} \qquad (n \geq 1).$$

This formula means that the generating function $F(x) := \sum F_n x^n$ satisfies the equation:

$$(1 - x - x^2) \cdot F(x) = 1,$$

and so

$$F(x) = \frac{1}{1 - x - x^2} = 1 + x + 2x^2 + 3x^2 + 5x^3 + \cdots.$$

Expanding $F(x)$, we have an explicit formula for Fibonacci numbers:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^{n+1} - \left(\frac{1 - \sqrt{5}}{2} \right)^{n+1} \right).$$

Example: Bell numbers $b(0), b(1), \cdots, b(n), \cdots$ are defined by

$$b(n) := \text{the number of equivalence relations on } \{1, \cdots, n\}$$

Then Bell numbers satisfy the recurrence formula

$$b(n+1) = \sum_{k=0}^{n} \binom{n}{k} b(k), \quad b(0) = 1.$$

Using this, we see that the generating function $B(x)$ of exponential type satisfies

$$B(x) := \sum_{n=0}^{\infty} b(n) \frac{x^n}{n!} = \exp(e^x - 1).$$

The concept of generating functions is a powerful tool for studying a sequence of numbers. If we have a generating function for a sequence $a_0, a_1, \cdots$, we can read many matters in it as follows:

(a) Explicit formula for a_n (e.g. Fibonacci numbers).

(b) Recurrence formula for a_n. For example, the exponential generating function $B(x) = \exp(e^x - 1)$ for Bell numbers $b(n)$ satisfies

$$B'(x) = e^x B(x),$$

which gives the recurrence formula for Bell numbers.

(c) Proof of identities.

We give an easy example. Binominal coefficients has the following generating function:

$$(1+x)^m = \sum_{i=0}^{m} \binom{n}{i} x^i.$$

Substituting it into the identity

$$(1+x)^m (1+x)^n = (1+x)^{m+n},$$

we have the well-known identity:

$$\sum_{i=0}^{k} \binom{m}{i} \binom{n}{k-i} = \binom{m+n}{k}$$

(d) Proof of congruence relation.

Let p be a prime. Then

$$(1+x)^{pn} \equiv (1+x^p)^n \pmod{p\boldsymbol{Z}[x]}.$$

Using the binomial theorem, we have the following well-known congruence:

$$\binom{pn}{pr} \equiv \binom{n}{r} \pmod{p}$$

(e) Proof of unimodality, convexity.

For example, observing the form of the generating function $(1+x)^n$ for binomial coefficients, we can prove that

$$\binom{n}{0} \leq \binom{n}{1} \leq \cdots \leq \binom{n}{[n/2]} = \binom{n}{[(n+1)/2]} \geq \cdots \geq \binom{n}{n-1} \geq \binom{n}{n}$$

$$\binom{n}{r}^2 > \binom{n}{r-1}\binom{n}{r+1}, \qquad 1 \leq r \leq n-1$$

(f) Statistic properties (eg. averages).

(g) Asymptotic formula

2. Exponential Series

Generating functions appear also in group theory. For example, Poincare series are used to study cohomology rings of finite groups. However, I think that we should further pursue the application of generating functions in group theory. We here give generating functions associated with the numbers of subgroups and homomorphisms of groups.

Let A be a finitely generated group. Then we define the exponential generating function of A as follows:

$$\begin{aligned} E(A;t) &:= \exp\left(\sum_{B \leq A} \frac{1}{(A:B)} t^{(A:B)}\right) \\ &= \exp\left(\sum_{n=0}^{\infty} \frac{s^n(A)}{n} t^n\right), \end{aligned}$$

where

$$s^n(A) := \sharp\{B \leq A | (A:B) = n\}$$

Then the following exponential formula holds:

Proposition (Wohlfahrt 1977):

$$E(A;t) = \sum_{n=0}^{\infty} |\mathrm{Hom}(A, S_n)| \frac{t^n}{n!}$$

This identity was repeatedly discovered by some mathematicians, but it seems that it was first proved by Wholfahrt ([Wo 77]). The recurrence formula for $h_n(A) := |\mathrm{Hom}(A, S_n)|$ that is equivalent to Wholfahrt's exponential formula is proved by Dey ([De 65]):

$$h_n(A) = \sum_{r \geq 1} \frac{(n-1)!}{(n-r)!} h_{n-r}(A) s^n(A).$$

This formula was applied to study the numbers of subgroups of given index in a free group and the modular group $\mathrm{SL}_2(\boldsymbol{Z})$ ([Ha 49]).

There are some interesting application of the exponential formula. We here state about the restricted Burnside problem. An application to Frobenius theorem is found in Section 4.

Let $f(q, m)$ be the supremum of the order of finite groups with m generators any of which elements have orders divisible by m. For example, it is well-known that $f(2, m) = 2^m$.

Restricted Burside Problem: $f(q, m) < \infty$?

This conjecture was reduced to the case where q is a power of a prime p by using Classification of Finite Simple Groups, and it was correctly proved by Zelmanov recently.

We can rewrite RBP by using generating functions as follows:

Define

$$\begin{aligned} L_{q,m}(t) &:= \log\left(\sum_{n=0}^{\infty} h_n t^n / n!\right) \\ h_n &:= |\mathrm{Hom}(B(q, m), S_n)| \\ &= \sharp\{(x_i) \in {S_n}^m | \langle x_1, \cdots x_m \rangle^q = 1\}, \end{aligned}$$

where $B(q, m)$ is a so-called Burnside group that is the largest group with m generators and satisfies the relation $X^q = 1$ for all elements X.

Then by the exponential formula, we have

$$\text{RBP} \iff L_{q,m}(t) \text{ is a polynomial.}$$

This statement does not mean that it can be used to prove RBP, but perhaps there is another approach to RBP.

3. The Artin-Hasse exponential function.

The Artin-Hasse exponential function is defined by

$$E_p(t) := E(\widehat{\boldsymbol{Z}}_p; t) = \exp\left(\sum_{i=0}^{\infty} p^{-i} t^{p^i}\right).$$

By the exponential formula for $A = \widehat{\boldsymbol{Z}}_p$, we have that

$$E_p(t) = \sum_{n=0}^{\infty} \frac{h_n}{n!} t^n,$$

where

$$h_n := |\mathrm{Hom}(\widehat{\boldsymbol{Z}}_p, S_n)| = \sharp\{p\text{-elements in } S_n\}.$$

By Frobenius theorem, we have that

$$h_n \equiv 0 \pmod{n!_p}.$$

This means that

$$E_p(t) \text{ converges in } \nu_p(t) > 0$$

as p-adic power series, where $\nu_p(p^e q) := e$. Note that $\nu_p(n!) = n!_p \approx n/(p-1)$. Thus the convergence region of the ordinal exponential function $\exp(t)$ is $\nu_p(t) > 1/(p-1)$.

Unfortunately, the Artin-Hasse exponential function does not satisfy the exponential law: $E_p(s+t) \neq E_p(s) \cdot E_p(t)$. However, Witt summation for Witt vectors makes the Artin-Hasse exponential function satisfy the exponential law.

A Witt vector $\boldsymbol{x}$ is a sequence of p-adic numbers:

$$\boldsymbol{x} = (x_0, x_1, x_2, \cdots).$$

The sum $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ of Witt vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ is inductively defined by

$$\sum_{i=0}^{n} p^i z_i^{p^{n-i}} = \sum_{i=0}^{n} p^i x_i^{p^{n-i}} + \sum_{i=0}^{n} p^i y_i^{p^{n-i}}, \qquad n = 0, 1, 2, \cdots.$$

Thus

$$z_0 = x_0 + y_0, \quad z_1 = x_1 + y_1 - \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i} {x_0}^{p-i}{y_0}^{i}, \quad \cdots.$$

We further extend the domain of the Artin–Hasse exponential function $E_p(x)$ to Witt vectors $\boldsymbol{x} = (x_0, x_1, x_2, \cdots)$ as follows:

$$E_p(\boldsymbol{x}) := \exp\left(\sum_{i=0}^{\infty} p^{-i} x_i^{p^{n-i}}\right).$$

Then we have the following formula:

Lemma

$$E_p(\boldsymbol{x}+\boldsymbol{y}) = E_p(\boldsymbol{x}) \cdot E_p(\boldsymbol{y}).$$

On the other hand, Dress and Siebeneicher discovered a surprising fact that the ring of Witt vectors is isomorphic to the (complete) Burnside ring of an infinite cyclic group ([DS 89]). It is a mistery why Witt vectors are related to cyclic groups in two way.

4. Frobenius theorem

In this section, we state Frobenius theorem and its generalizations.

Theorem (Frobenius 1903, 1907):

$$\sharp\{x \in G \mid x^n = 1\} \equiv 0 \bmod \gcd(n, |G|).$$

Some important research around this theorem were published recently ([BT 88]). Furthermore, it is noteworthy to write here that H.Yamaki solved Frobenius conjecture correctly.

We note that Frobenius theorem is extended as follows:

Theorem ([Yo ??]): *Let A be a finite group and G a finite group. Then the number of homomorphisms from A to G satisfies the following congruence:*

$$|\mathrm{Hom}(A, G)| \equiv 0 \quad \gcd(|A|, |G|).$$

The proof of this theorem is elementary but not short as other theorems in finite group theory. Since there is a bijective correspondence between $\mathrm{Hom}(C_n, G)$ and the set $\{x \in G \mid x^n = 1\}$, this theorem implies the ordinary Frobenius theorem.

Furthermore, when G is a symmetric group S_n, there is another proof by using the exponential formula ([DY ??]). To do it, we study the generating function

$$E(A;t) := \sum_{n\geq 0} \frac{h_n}{n!} t^n,$$

where $h_n := |\mathrm{Hom}(A, S_n)|$, and then we deduce the proof of the theorem to the ordinary Frobenius theorem (for cyclic groups) and the following lemma for abelian p-groups:

Lemma: *Let A be an abelian group of order p^n and let $s_i(A)$ denote the number of subgroups of A of order p^i. Then for $0 \leq i \leq [(n+1)/2]$,*

$$s_i(A) \equiv s_{i-1}(A) \qquad \mathrm{mod}\ p^i.$$

Remark: The unimodality

$$1 = s_0(A) \leq s_1(A) \leq \cdots s_{[n/2]} = s_{[(n+1)/2]} \geq \cdots \geq s_{n-1} \geq s_n$$

was recently proved by L.M.Butler ([Bu 87]).

It is natural to ask the following generalization of the above Frobenius type theorem for a non-abelian A:

Conjecture 1: (Asai-Yoshida [AY ??]): For finite groups A and G,

$$|\mathrm{Hom}(A, G)| \equiv 0 \bmod \gcd(|A/A'|, |G|),$$

where A' denotes the commutator group of A.

This conjecture is still unsolved, but a weak result holds:

Theorem ([AY ??]):

$$|\mathrm{Hom}(A, G)| \equiv 0 \bmod \gcd(|(A/A')/\Phi(A/A')|),$$

where $\Phi(A/A')$ denotes the Frattini subgroup of A/A'.

There is more general conjecture than the above one:

Conjecture 2: ([AY ??]): *Assume that a finite group A acts on another finite group G. Then*

$$|Z^1(A,G)| \equiv 0 \bmod \gcd(|A/A'|, |G|),$$

where $Z^1(A,G)$ is the set of cocycles $\zeta : A \longrightarrow G$ (i.e. $\zeta(ab) = \zeta(a) \cdot {}^a\zeta(b)$).

It is known that if Conjecture 2 for any abelian p-group A and any p-group G is correct, then Conjecture 1 is also correct for all finite groups.

5. Asymptotic Properties for $\nu_p(h_n(A))$

As in Section 3, we put $h_n := h_n(A) := |\mathrm{Hom}(A, S_n)|$, and we let $\nu_p(n)$ denote the p-part of an integer n. We are interested to the asymptotic behavior of $\nu_p(h_n(A))$.

Using Frobenius-Yoshida theorem in the preceding section, we have the lower bound of $\nu_p(h_n(A))$ for abelian group A:

Theorem (Frobenius–Yoshida): *Let A be a finite abelian group. Then*

$$\nu_p(h_n(A)) \geq \min(\nu_p(|A|)), \nu_p(n!)).$$

In particular,

$$\nu_p(h_n(A)) \geq \nu_p(|A|) \qquad \text{for large } n.$$

We consider

$$h_n(C_p) = \sharp\{x \in S_n \mid x^p = 1\}$$

The generating function of this sequence $h_n(C_p)$, $n = 0, 1, 2, \cdots$ is

$$E(C_p;t) = \sum_{n=0}^{\infty} \frac{h_n(C_p)}{n!} t^n = \exp\left(t + \frac{t^p}{p}\right)$$

and the recurrence formula is

$$h_n(C_p) = h_{n-1}(C_p) + \frac{(n-1)!}{(n-p)!} h_{n-p}(C_p), \qquad n \geq 1.$$

Using these formulas, an assymptotic formula was proved by Moser–Wyman (1955) and Wilf (1986):

$$h_n(C_p) \approx \frac{(n-n/p)!}{\sqrt{2n\pi(p-1)}} \exp(n^{1/p}).$$

However, to calculate $\nu_p(h_n(C_p))$ is a very hard problem. For example, I do not know when $h_p(C_p) = 1 + (p-1)!$ is divisible by p^2. By a long calculation on the generating function of $h_n(C_p)$, we can prove the following lower bound:

Theorem ([DY ??]):

$$\nu_p(h_n(C_p)) \geq \left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right].$$

In many cases $\nu_p(h_n(A))$ seems to increse asymptotically in proporsion to n. Thus to make the following conjecture is natural:

Conjecture: For any finite group A, define

$$R_p(A) := \lim_{n\to\infty} \nu_p(h_n(A))/n.$$

Then $R_p(A)$ is a rational number.

Example:

$$\begin{aligned} R_p(C_p) &= p^{-1} - p^{-2}, \\ R_p(C_{p^2}) &= p^{-1} + p^{-2} - 2p^{-3}. \end{aligned}$$

The second formula is essentially proved by Y.Takegahara.

6. Eulerian series

In this section, we study a q-analogue of the exponential forumula. Let $F := \mathbf{F}_q$ and A a finite group such that $(|A|, q) = 1$.Furthermore, let $V_1, \cdots, V_r$ be all irreducible FA-modules (up to isomorphisms) with

$$D_i := \mathrm{End}_{FA}(V_i), \qquad q_i := |D_i|,$$

so that D_i is a finite field of order q_i.

We now define the q-exponential series by

$$\mathrm{Exp}_{A,q}(t) := \sum_{n=0}^{\infty} \frac{|\mathrm{Hom}(A, \mathrm{GL}(n, q))|}{|\mathrm{GL}(n, q)|} t^n$$

Then we have a q-exponential formula:

Theorem : *Under the above notation,*

$$\begin{aligned}\mathrm{Exp}_{A,q}(t) &:= \sum_{V}{}' \frac{t^{\dim V}}{|\mathrm{Aut}_{FA}(V)|} \\ &= \prod_{i} \sum_{n=0}^{\infty} \frac{t^{\dim V_i}}{|\mathrm{GL}(n, q_i)|}\end{aligned}$$

If $|A|$ divides $q-1$, then F is a splitting field for A, and so $q_i = q$. Thus by using Roger–Ramanujan's identity ([An 76]), we have the following infinite product expansion:

Corollary: *If* $|A|$ *divides* $q - 1$, *then*

$$\mathrm{Exp}_{A,q}(1) = \left(\prod_{n=0}^{\infty} \frac{1}{(1 - q^{-5n-1})(1 - q^{-5n-4})} \right)^r$$

It looks strange that $\mathrm{Exp}_{A,q}(1)$ depends only on the number r of conjugacy classes in A.

Using the above theorem, we can prove that a special case of Conjecture 1 in Section 4 is correct:

Theorem: If $|A/A'|$ divides $q-1$ and $n \geq 1$, then

$$|\mathrm{Hom}(A, \mathrm{GL}(n,q))| \equiv 0 \pmod{|G/G'|}$$

7. Congruence zeta function

There is another kind of generating function related to the number of homomorphisms from a fixed finite group to general linear groups. We fix a finite group A, a natural number n and a power q of a prime. Then we define the congruence zeta function as follows:

$$\begin{aligned} N_r &:= |\mathrm{Hom}(A, \mathrm{GL}(n, q^r))| \\ Z(A;t) &:= \exp\left(\sum_{r=1}^{\infty} \frac{N_r}{r} t^r\right) \end{aligned}$$

It is well-known that $Z(A;t)$ is a rational function (Dwork).

Furthermore, Frobenius–Yoshida's theorem in Section 4 implies the following congruence:

Theorem: *Let A be an abelian group such that $(|A|, q) = 1$. Then*

$$\deg Z(A;t) \equiv 0 \qquad \mathrm{mod}\ \gcd(|A|, |\mathrm{GL}(n,q)|)$$

However, it seems that the degree of $Z(A;t)$ increase again asymptotically in proporsion to n. Furthermore, zeros and poles are interesting forms.

Example: Let l be a prime divisor of $q-1$. Then $\deg Z(C_l;t) = -l^n$.

References

[An 76] G.E.ANDREWS, "The Theory of Partitions ", in *Encyclopedia of Mathematics and its Applications* vol. 2, 1976.

[AY ??] T.ASAI–T.YOSHIDA, $|\mathrm{Hom}(A,G)|$ (II), *J.Algebra*, accepted.

[Br 75] K.BROWN, Euler characteristics of groups : The p-fractional part, *Invent. Math.* **29** (1975), 414–430.

[BT 88] K.BROWN–J.THÉVENAZ, A generalization of Sylow's third theorem, *J. Algebra* **115** (1988), 414–430.

[Bu 87] L.M.BUTLER, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc.* **101** (1987), 771–779.

[DS 89] A.W.M.DRESS–C.SIEBENEICHER, The Burnside ring of the infinite cyclic group and its relations to the necklace albebra, λ-rings, and the universal ring of Witt vectors, *Acvances in Algebra*, **78** (1989), 1–41.

[GIR 79] C.GODSIL–W.IMRICH–R.RAZEN, On the number of subgroups of given index in the modular group, *Monasch Math.*, **87** (1979), 1–8.

[Ha 49] M.HALL, Subgroups of finite index in free groups, *Canad. J. Math.*, **1** (1949). 187–190.

[Ge 91] 「現代の母関数」(1990 鳥取におけるセミナー), 日比・若山編, 1991.

[Ko 78] N.KOBLITZ, "p-adic Numbers, p-adic Analysis, and Zeta–Functions", Springer, 1977.

[St 86] R.P.STANLEY, "Enumerative Combinatorics", Wadsworth–Brooks / Cole, 1986.

[Va 85] M.R.VAUGHAN-LEE, The restricted Burnside problem, *Bull. London Math. Soc.*, **17** (1985), 113–133.

[Wo 77] K.WOHLFAHRT, Über einen Satz von Dey und die Modulgruppe, *Arch, Math.* **29** (1977), 455–457.

[Yo ??] T.YOSHIDA, $|\mathrm{Hom}(A,G)|$, *J.Algebra*, in printing.