Integer valued functions on the integers*

Karl W. Gruenberg
University of London

We shall be concerned with the set $\mathcal{X}$ of functions ϕ defined on the non-negative integers $\mathbb{Z}_{\geq 0}$ and with values in $\mathbb{Z}$. The ring structure on $\mathbb{Z}$ enables us to make $\mathcal{X}$ into a ring:

$$(\phi + \psi)(n) = \phi(n) + \psi(n) \quad \text{and} \quad (\phi\psi)(n) = \phi(n)\psi(n);$$

the constant function with value 1 is the identity of $\mathcal{X}$.

Such functions arise in every part of mathematics. Their importance stems from the fact that if a given situation gives rise to such a function, then its properties often yield structural information about the original mathematical situation.

Let me pick three examples and since I am an algebraist they are all drawn from algebra.

(1) Let R be a commutative noetherian local ring. "Noetherian" means that R satisfies the maximal condition on ideals and "local" means that R has exactly one maximal ideal, call it I. For example, if p is a prime number, the subring $\mathbb{Z}_{(p)}$ of the rational numbers $\mathbb{Q}$ consisting of all ratios of integers a/b, with b prime to p, is such a ring, the maximal ideal being $p\mathbb{Z}_{(p)}$.

By the maximality of I, $R/I = K$ is a field and by the noetherian property, each I^r is finitely generated as an ideal. Hence each I^r/I^{r+1} is a finite dimensional vector space over K. Then

$$r \mapsto \dim_K I^r/I^{r+1}$$

is a function in $\mathcal{X}$.

---

* Written version of invited lecture delivered to the Singapore Mathematical Society and the Department of Mathematics, National University of Singapore, on 3 April 1989. Professor Gruenberg was visiting the National University of Singapore as External Examiner in Mathematics.

(2) Let G be a group with a given finite set of generators S. Then every element g in G can be expressed in the form

$$g = s_1^{\epsilon_1} \dots s_n^{\epsilon_n},$$

where $s_i \in S$ and $\epsilon_i = \pm 1$. We call n the length of this expression. Of course, our element g may have many different expressions, so n is not determined by g. For each $n \in \mathbb{Z}_{\geq 0}$, let $G(n)$ be the set of all g in G that have an expression of length $\leq n$. ($G(0) = \{1\}$.) Since S is finite, $G(n)$ is finite and we write $l(n)$ for the cardinality of $G(n)$. Then l is a function in $\mathcal{X}$.

(3) Let K be a field, G a finite group and A a finitely generated KG-module. We choose a finitely generated projective resolution of A over KG:

$$\cdots \to P_{i+1} \to P_i \to \cdots \to P_1 \to P_0 \to A \to 0.$$

This means that each P_i is a finitely generated projective KG-module (a projective module is a direct summand of a free module) and the displayed sequence is an exact sequence of modules (meaning that the image of each incoming arrow is the kernel of the outgoing arrow).

Since G is finite, every finitely generated KG-module is a finite dimensional vector space over K. Hence

$$n \mapsto \dim_K P_n$$

is a function in $\mathcal{X}$.

We shall reexamine all these examples later. But now we turn to general observations about our ring $\mathcal{X}$. The simplest functions that live in $\mathcal{X}$ are the polynomially defined ones. We say ϕ is *polynomially defined* if there is a polynomial $f(X) \in \mathbb{Q}[X]$ so that $\phi(n) = f(n)$ for all $n \geq 0$. Note that $f(X)$ need not have integer coefficients: for example, with k any positive integer,

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!}$$

takes only integral values when X is made integral. If $\mathcal{P}$ denotes the set of all polynomially defined functions, then $\mathcal{P}$ is a subring of $\mathcal{X}$ and we now claim that every function in $\mathcal{P}$ can be constructed from the above binomial polynomials:

Proposition 1. *The polynomial* $\binom{X}{k}$ *for* $k \geq 0$ *(here* $\binom{X}{0}$ *means 1) form a* $\mathbb{Q}$*-basis of* $\mathbb{Q}[X]$*, and they additively generate (a group isomorphic to)* $\mathcal{P}$.

Proof. The $\mathbb{Q}$-basis property is immediate by an induction on degree if we note that

$$\binom{X}{k} = \frac{X^k}{k!} + g(X),$$

where $^\circ g$ (the degree of g) is strictly smaller than k.

We prove the second assertion also by induction on degree. So let ϕ in $\mathcal{P}$ be given by the polynomial $f(X)$ and (using the first part of the Proposition) suppose

$$f(X) = \sum_{k=0}^{r} a_k \binom{X}{k},$$

where $a_k \in \mathbb{Q}$. We need to show each a_k is an integer.

For any polynomial $g(X)$, let

$$\delta g(X) = g(X+1) - g(X).$$

Then $\delta\binom{X}{k} = \binom{X}{k-1}$ and so

$$\delta f(X) = \sum_{k=1}^{r} a_k \binom{X}{k-1}.$$

Now δf has smaller degree than f and is still integral valued at all $n \geq 0$. So by induction each of $a_1, \ldots, a_r$ is in $\mathbb{Z}$. Since

$$a_0 = f(X) - \sum_{k=1}^{r} a_k \binom{X}{k}$$

and the right hand side takes only integral values, so a_0 is also in $\mathbb{Z}$. □

Polynomially defined functions occur rarely. A slight generalization leads to functions that appear frequently. Let q be a positive integer. We say ϕ in $\mathcal{X}$ is *polynomial on residue classes* $\bmod q$ (PORC $\bmod q$) if there exist polynomials $f_0(X), \ldots, f_{q-1}(X)$ in $\mathbb{Q}[X]$ such that, for every $0 \leq r < q$ and $n \in \mathbb{Z}$,

$$\phi(nq + r) = f_r(n).$$

Of course, every integer can be written in the form $nq+r$. Note also that if $\phi \in \mathcal{P}$, then ϕ is PORC mod 1.

We say two functions ϕ, ψ are *ultimately equal* if there exists an integer N so that $n \geq N$ implies $\phi(n) = \psi(n)$ and we write $\phi \sim \psi$. The function ϕ is ultimately PORC mod q if there exists a PORC mod q function ψ so that $\phi \sim \psi$.

To every ϕ in $\mathcal{X}$ we may attach a formal power series

$$P(\phi, X) = \sum_{n \geq 0} \phi(n) X^n .$$

This is often called the *Poincaré series* for ϕ. Note that $\phi \sim \psi$ if, and only if,

$$P(\phi, X) - P(\psi, X) \in \mathbb{Z}[X].$$

The Poincaré series of PORC functions have a particularly nice form:

Proposition 2. *The function ϕ is ultimately PORC* mod q *if, and only if,*

$$P(\phi, X) = \frac{g(X)}{(1-X^q)^t},$$

where $g(X) \in \mathbb{Z}[X]$ and t is a positive integer.

Proof. Assume first that $\phi \sim \psi$ with ψ PORC mod q and given by the polynomials $f_0, \ldots, f_{q-1}$. It will suffice to show that $P(\psi, X)$ has the required form. Now

$$\begin{aligned} P(\psi, X) &= \sum_{m \geq 0} \psi(m) X^m \\ &= \sum_{r=0}^{q-1} \sum_{n \geq 0} \psi(nq+r) X^{nq+r} \\ &= \sum_{r=0}^{q-1} X^r \Big(\sum_{n \geq 0} f_r(n) X^{nq} \Big). \end{aligned}$$

Hence it will suffice to show $\sum_{n \geq 0} f_r(n) X^{nq}$ has the required form, for every r.

By Proposition 1,

$$f_r(X) = \sum_{i=0}^{d} a_i \binom{X}{i},$$

with each $a_i \in \mathbb{Z}$ and $d = {}^\circ f_r$. So we are reduced to proving that, for each i, $\sum_{n\geq 0} \binom{n}{i} X^{nq}$ has the required form. We have

$$\frac{1}{(1-X^k)^s} = \sum_{n\geq 0} \binom{-s}{n} (-X^k)^n$$

and

$$\binom{-s}{n} = (-1)^n \frac{s(s+1)\cdots(s+n-1)}{n!}$$

$$= (-1)^n \frac{(n+s-1)!}{n!(s-1)!}$$

$$= (-1)^n \binom{n+s-1}{s-1}.$$

Thus

$$\frac{1}{(1-X^k)^s} = \sum_{n\geq 0} \binom{n+s-1}{s-1} X^{kn}. \tag{1}$$

Using also that $\binom{n}{i} = 0$ if $n < i$, we deduce

$$\sum_{n\geq 0} \binom{n}{i} X^{nq} = \sum_{m\geq 0} \binom{m+i}{i} X^{mq+iq}$$

$$= \frac{X^{iq}}{(1-X^q)^{i+1}},$$

as required.

Assume now conversely that

$$P(\phi, X) = \frac{g(X)}{(1-X^q)^t}.$$

By (1)

$$\frac{1}{(1-X^q)^t} = \sum_{n\geq 0} \binom{n+t-1}{t-1} X^{qn},$$

whence the coefficient function is PORC mod q with polynomials

$$\binom{X+t-1}{t-1}, 0, 0, \cdots, 0.$$

If $f(X)$ is a polynomial with integer coefficients of degree $< q$, say

$$f(X) = \sum_{i=0}^{q-1} b_i X^i,$$

then

$$\frac{f(X)}{(1-X^q)^t} = \sum_{i=0}^{q-1} \sum_{n \geq 0} \binom{n+t-1}{t-1} b_i X^{qn+i}$$

and so this is the Poincaré series of a function PORC mod q with polynomials $b_i \binom{X+t-1}{t-1}$, $0 \leq i < q$. Now write our given polynomial $g(X)$ as

$$g(X) = \sum_{i \geq 0} g_i(X)(1-X^q)^i,$$

where $°g_i < q$. (This is really a finite sum.) Then

$$\frac{g(X)}{(1-X^q)^t} = h(X) + \sum_{i=0}^{t-1} \frac{g_i(X)}{(1-X^q)^{t-i}}. \tag{2}$$

The second term on the right hand side of (2) is PORC mod q, as we proved above, and hence the left hand side is ultimately PORC mod q. □

Note that the integer t in Proposition 2 can be taken to be $1+d$, where $d = \max\{°f_0, °f_1, \ldots, °f_{q-1}\}$. This follows from our proof.

Functions that are ultimately PORC grow only polynomially. To be precise, let us define ϕ to be of *polynomial growth* $c \geq 0$ if there exists a positive real number a and a positive integer N so that $n \geq N$ implies $|\phi(n)| \leq an^{c-1}$ and c is the smallest such integer.

Proposition 3. *If ϕ is ultimately PORC* mod q, *given by* $f_0, \ldots, f_{q-1}$ *and d is the maximum of the degrees of* $f_0, \ldots, f_{q-1}$, *then ϕ is of polynomial growth* $d+1$.

Proof. Suppose ϕ becomes PORC mod q at N. If $n \geq N$ and $n = kq + r$, then

$$|\phi(n)| = |f_r(k)| \leq \left(\sum_{i=0}^{d_r} |a_i| \right) k^{d_r},$$

where $f_r(X) = \sum_{i=0}^{d_r} a_i X^i$. If $\sum_{i=0}^{d_r} |a_i| = A_r$, define $a = \max(A_0, \ldots, A_{q-1})$. Then $|\phi(n)| \leq an^d$ for all $n \geq N$.

Now assume $|\phi(n)| \leq an^{c-1}$ for all $n \geq N$ and let d be the degree of f_r. Then

$$|f_r(k)| = |\phi(kq + r)| \leq a(kq + r)^{c-1}$$

for all $k \geq K$ say. If $g(X)$ is the polynomial $a(qX + r)^{c-1}$, then $^\circ g = c - 1$ and $|f_r(k)| \leq g(k)$ for all $k \geq K$. This implies $^\circ f_r \leq {}^\circ g$, i.e., $d \leq c-1$. □

The converse of Proposition 3 is false. For example, let

$$\phi(n) = \begin{cases} n & \text{if } n \text{ is not a prime} \\ 0 & \text{if } n \text{ is a prime.} \end{cases}$$

Then $\phi(n) \leq n^{2-1}$ so that ϕ has polynomial growth 2. But if ϕ were PORC mod q above, say, N with polynomials $f_0, \ldots, f_{q-1}$, then $qk+r \geq N$ implies

$$f_r(k) = \phi(qk + r)$$

and the right hand side is 0 whenever $qk + r$ is a prime. By Dirichlet's famous theorem, $\mathbb{Z}q + r$ contains infinitely many primes and so $f_r(X)$ has infinitely many roots, an impossibility.

Let us now return to our three examples.

(1) Recall that R has unique maximal ideal I and our function is $\phi(n) = \dim_K I^n / I^{n+1}$. The basic theorem here is that the associated Poincaré series is

$$P(\phi, X) = \frac{g(X)}{(1 - X)^t},$$

where, by cancellation, we may assume $1 - X$ is not a factor of $g(X)$. Then t is the *Krull dimension* of the local ring R (this means that t is the supremum of the lengths of all chains of prime ideals in R). Thus ϕ is ultimately polynomially defined and the polynomial in question is called the *Hilbert polynomial* of R.

If $R = \mathbb{Z}_{(p)}$, $P(\phi, X) = \frac{1}{1-X}$ and the Hilbert polynomial is 1.

A good account of this theory is in [1], Chapter 11.

(2) In this example $G = \langle S \rangle$ with S finite and $l(n)$ is the number of elements in the group G that can be written as an S-word of length $\leq n$. An important theorem of Gromov [6] asserts that l has polynomial growth if, and only if, G has a nilpotent subgroup of finite index. Very recently Grunewald has shown that if l is of polynomial growth it need not be ultimately PORC. (There is a beautiful proof of Gromov's theorem by methods of non-standard analysis, due to van den Dries and Wilkie [4].)

Grunewald's example is a type of Heisenberg group. Let H_k (the k-th Heisenberg group) be the group with generators $x_1, \ldots, x_k, y_1, \ldots, y_k; z$ subject to the relations

$$[x_i, y_i] = z \qquad \text{is central,}$$
$$[x_i, y_j] = 1 \qquad \text{if} \quad i \neq j,$$

the x's commute and the y's commute.

Take $S = \{x_1, \ldots, x_k, y_1, \ldots, y_k\}$. Then H_1 is the free nilpotent group of rank 2 and class 2 and here it is known that

$$P(l, X) = \frac{g(X)}{(1 - X^{12})^5}.$$

This was conjectured by R. Bödeker and proved independently by M. Shapiro and B. Weber. However, Grunewald has proved that l for H_2 and S is not ultimately PORC, nor even rational.

(3) For our KG-module A we choose a projective resolution

$$\cdots \to P_1 \to P_0 \to A \to 0$$

with the property that for each i, the image of P_i in P_{i-1} contains no projective direct summand. Such a resolution always exists and is, in a sense, the tightest resolution possible. It is also unique (to within isomorphism). The claim now is that $n \mapsto \dim_K P_n$ is ultimately PORC.

This result depends on two theorems:

(i) $\operatorname{Ext}_{KG}(K, K)$ is a graded noetherian K-algebra (Evens [5]) and for any KG-module M, $\operatorname{Ext}_{KG}(K, M)$ is a finitely generated graded module over $\operatorname{Ext}_{KG}(K, K)$;

(ii) if V is a finitely generated graded module over a graded commutative noetherian K-algebra Λ, then $n \mapsto \dim_K V_n$ is ultimately PORC. This result is nowadays usually known as the Hilbert-Serre theorem. A special case of it lies behind the theorem on local rings in example (1). Cf [1].

Putting (i) and (ii) together shows the function

$$n \mapsto \dim_K \operatorname{Ext}^n_{KG}(K, M)$$

is ultimately PORC, whence so is

$$n \mapsto \dim_K \operatorname{Ext}^n_{KG}(A, B)$$

for any KG-modules A, B (because

$$\operatorname{Ext}_{KG}(A, B) \simeq \operatorname{Ext}_{KG}(K, \operatorname{Hom}_K(A, B))).$$

Now a relatively elementary argument shows

$$\dim_K P_n = \sum_S r_S \dim_K \operatorname{Ext}^n_{KG}(A, S),$$

where S runs through all simple KG-modules and each $r_S \in \mathbb{Z}_{>0}$. The required conclusion that $n \mapsto \dim P_n$ is ultimately PORC follows because the set of functions ultimately PORC is closed under addition (in fact, it is a subring of $\mathcal{X}$).

These ideas go back to Swan [8]. A good introduction to this material is Carlson's little book [3].

In preparing the written version of this lecture I have been helped by a letter from Fritz Grunewald and a comment by Aidan Schofield.

In addition to the literature already cited, I should mention the comprehensive survey by Babenko [2] of growth functions in algebra and algebraic topology.

References

[1] M.F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley 1969.

[2] I. K. Babenko, Problems of growth and rationality in algebra and topology, *Uspekhi Mat. Nauk* **41: 2**(1986) 95-142 (*Russian Math. Surveys* **41: 2**(1986) 117-175).

[3] J. F. Carlson, Module varieties and cohomology rings of finite groups, *Vorlesungen der Univ. Essen* **13**(1985).

[4] L. van den Dries and A. J. Wilkie, Gromov's theorem on groups of polynomial growth and elementray logic, *J. Algebra* **89**(1984) 349-374.

[5] L. Evens, The cohomology ring of a finite group, *Trans. Amer. Math. Soc.* **101**(1961) 224-239.

[6] M. Gromov, Groups of polynomial growth and expanding maps, *Publ. Math. IHES* **53**(1981) 53-78.

[7] M. Shapiro, A geometric approach to the almost convexity and growth of some nilpotent groups, *Math. Annalen* (to appear).

[8] R. G. Swan, Groups with no odd dimensional cohomology, *J. Algebra* **17**(1971) 401-3.

[9] B. Weber, Zur Rationalität polynomialer Wachstumsfunktionen, *Bonner Math. Schr.* **197**(1989).