Witt vectors, the Grothendieck Burnside ring, and Necklaces

Barry Dayton

January, 1996

It has always amazed me how the most abstract ideas in mathematics have been applied to the art of counting things. Examples that come to mind in commutative algebra include Reisner's use of Cohen Macaulay rings to count faces of sphere triangulations and the use of Hochschild homology by Bayer and Diaconis to solve problems in card shuffling. It has never been clear to me whether this is because underneath all our abstractions, mathematics really is just about counting things or whether this phenomenon is merely due to the large egos of combinatorists – they want us to *think* mathematics is about counting things.

In this note I explore some more connections between commutative algebra and counting techniques. These connections lend credence to my latter supposition, for this connection has apparently led to no new combinatorics, all the formulas about necklaces were well known long before, and the thrust of the published papers [8, 5, 6] seems to be that somehow the combinatorics improves the algebra, an idea of which I am skeptical. In this note I take an opposite point of view from [8], I assume the algebra is reasonably familiar and derive the combinatorics from the algebra.

1 Witt Vectors

The preceding ideas can be axiomitized by the modern idea of (big) Witt vectors. It is generally accepted that these Witt vectors made their official debut in the paper by Cartier [4] even though they appear to have been discovered much earlier by E. Witt, for instance they had previously appeared in print in the form of a series of exercises in S. Lang's textbook [7].

Let R be a commutative ring with unit, which I will view as a commutative **Z**-algebra. As a set we define $W(R)$ to be the set of unitary power series in R, i.e $W(R) = \{a(t) = 1 + a_1t + a_2t^2 + \cdots \in R[[t]]\}$. The addition in $W(R)$ will be the usual multiplication of power series. I will use the usual multiplicative notation, so that for $a(t), b(t) \in W(R)$, $a(t)b(t)$ is the "sum", $\frac{a(t)}{b(t)}$ is the "difference", and in an expression such as $(1-t)^r$, r is the "coefficient".

Central to our discussion is the *ghost map*. This is the map $W(R) \to tR[[t]]$ given by

$$gh(a) = -t\frac{a'(t)}{a(t)} = \frac{d}{dt}\log a(t)$$

If $gh(a(t)) = f_1t + f_2t^2 + \cdots$ we call f_i the ith ghost component of a or $gh_i(a)$. I think it is useful to recognize that the connection between the components of $a(t) \in W(R)$ and the ghost components is given by the classical *Newton's Identities.*

$$f_n + f_{n-1}a_1 + f_{n-2}a_2 + \cdots + f_1a_{n-1} + na_n = 0 \tag{1}$$

The ghost map is a homomorphism of the additve groups of $W(R)$ and $tR[[t]]$, but rather than viewing $tR[[t]]$ as an ideal of $R[[t]]$ I will view it as the product $\prod_{i=1}^{\infty} R$ via the map $f_1t + f_2t^2 + \cdots \mapsto (f_1, f_2, f_3, \ldots)$ and thus addition is the same but multiplication is given by

$$(f_1t + f_2t^2 + \cdots) * (g_1t + g_2t^2 + \cdots) = (f_1g_1)t + (f_2g_2)t^2 + \cdots \tag{2}$$

If R has no **Z**-torsion (i.e. $nr = 0$ implies $r = 0$ for $n \in \mathbf{Z}, n \neq 0, r \in R$) then it is easily seen from Newton's Identities that gh is injective and if R contains the rationals **Q** then gh is bijective. In this latter case the ring structure on $tR[[t]]$ given by (2) determines a ring structure on $W(R)$ so that $gh : W(R) \to tR[[t]]$ is an isomorphsim.

I am more interested in the case that $R = \mathbf{Z}$ but it is in fact true in general that there is a multiplication in $W(R)$ which makes gh a homomorphism of rings. There are probably more arguments for this than there are authors who have written about Witt vectors (see, for example, [1, 2, 3]) but I must stick in my own two cents worth with a sketch of my own favorite argument. It is clearly enough to establish this for the ring $\mathbf{Z}[\{a_i\}_{i=1}^{\infty}, \{b_i\}_{i=1}^{\infty}, \{c_i\}_{i=1}^{\infty}]$ of polynomials in infinitely many indeterminants, so we can assume that R is an integral domain with no **Z**-torsion. Thus gh is injective and one only needs to show that if f, g are in the image of gh then fg is also in the image. Now Newton's Identities tell us that the nth ghost component $gh_n(a)$ depends only on the first n components of a and thus by a limit argument in the appropriate topology it is enough to show that given $a, b \in W(R)$ given any positive integer n there is a $c \in W(R)$ with $gh_i(c) = gh_i(a)gh_i(b)$ for $i \leq n$. But imbed R in an algebraically closed field K and consider the polynomials $p(t) = 1 + a_1t + \cdots + a_nt^n, q(t) = 1 + b_1t + \cdots + b_nt^n \in K[t]$. Suppose these have roots $\{\alpha_1, \ldots, \alpha_n\}, \{\beta_1, \ldots, \beta_n\}$ respectively in K. By the classical theory of symmetric functions the polynomial $u(t) = 1 + c_1t + \cdots + c_{n^2}t^{n^2}$ which has roots $\{\alpha_i\beta_j | 1 \leq i, j \leq n\}$ has coefficients in R. But the original content of Newton's Identities was that $gh_i(p) = \alpha_1^{-i} + \cdots + \alpha_n^{-i}$ etc. so that for $1 \leq i \leq n$ $gh_i(a)gh_i(b) = gh_i(p)gh_i(q) = gh_i(u)$ and thus $c = 1 + c_1t + c_2t^2 + \cdots$ is our desired Witt vector.

Denoting multiplication by $*$ it is seen

$$(1 - rt^m) * (1 - st^n) = (1 - r^{n/d}s^{m/d}t^{mn/d})^d, d = (m, n) \tag{3}$$

where (m, n) is the greatest common divisor. This can be checked by noting that

$$gh(1 - rt^m) = mrt^m + mr^2t^{2m} + mr^3t^{3m} + \cdots$$

In particular $1 - t$ is the multiplicative identity. (The astute reader will note that this differs from some authors such as [8, 2] where $(1 - t)^{-1}$ is the multiplicative identity.)

In general $W(R)$ is not an R-algebra, however there is a fairly common type of ring for which $W(R)$ is an R-algebra. This is a *binomial ring,* i.e. a ring with no **Z**-torsion in which for each $r \in R$ and positive integer n,

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

is an element of R. For example the ring of integers and any ring containing **Q** is a binomial ring. For a binomial ring there is a map $\lambda : R \to W(R)$ given by

$$\lambda(r) = (1-t)^r = \sum_{n=0}^{\infty} (-1)^n \binom{r}{n} t^n$$

which imbeds R as a subring of $W(R)$. More generally

$$(1-t^m)^r = \sum_{n=0}^{\infty} (-1)^n \binom{r}{n} t^{mn}$$

is an element of $W(R)$. We note that

$$gh((1-t^m)^r) = mrt^m + mrt^{2m} + mrt^{3m} + \cdots$$

which, incidentally, gives a proof (letting $m = 1$) that λ is an injective ring homomorphism.

For our purposes, the central result of this section is essentially the first proposition of [8, p. 113]. I remind the reader that $\prod$ below refers to the "sum" in $W(R)$.

Proposition 1 *Let R be a binomial ring. Then each $a \in W(R)$ can be written uniquely in the form*

$$a = \prod_{m=1}^{\infty} (1-t^m)^{r_m}$$

for appropriate $r_1, r_2, r_3, \ldots \in R$.

Sketch of Proof: Suppose $gh(a) = f_m t^m + f_{m+1} t^{m+1} + \cdots$ for some $m \geq 1$. It follows easily from Newton's identities that f_m is divisible by m in R so then $a(1-t^m)^{-(f_m/m)} \in W(R)$ and $gh_i(a(1-t^m)^{-(f_m/m)}) = 0$ for all $i \leq m+1$. Thus successively "subtracting" Witt vectors of the form $(1-t^m)^{r_m}$ from a produces a sequence of elements in $W(R)$ converging to the zero Witt vector. An appropriate limit argument would clean up the details.

Example 2 I illustrate the constructive approach above by calculating the decomposition of the Witt vector $a = 1 - 5t \in W(\mathbf{Z})$. I first calculate

$$gh(a) = 5t + 25t^2 + 125t^3 + 625t^4 + 3125t^5 + 15625t^6 + \cdots$$

I now note that $gh((1-t)^5) = 5t + 5t^2 + 5t^3 + \cdots$ so

$$gh(a(1-t)^{-5}) = 20t^2 + 120t^3 + 620t^4 + 3120t^5 + 15620t^6 + \cdots$$

But $gh(((1-t^2)^{10}) = 20t^2 + 20t^4 + 20t^6 + \cdots$ so

$$gh(a(1-t)^{-5}(1-t^2)^{-10}) = 120t^3 + 600t^4 + 3120t^5 + 15600t^6 + \cdots$$

Next $gh((1-t^3)^{40} = 120t^3 + 120t^6 + \cdots$ so

$$gh(a(1-t) - 5(1-t^2)^{-10}(1-t^3)^{-40}) = 600t^4 + 3120t^5 + 15480t^6 + \cdots$$

Finally as $600/4 = 150, 3120/5 = 624$ and $15480/6 = 2580$ I conclude that

$$a = (1-t)^5(1-t^2)^{10}(1-t^3)^{40}(1-t^4)^{150}(1-t^5)^{624}(1-t^6)^{2580}\cdots$$

Assuming that $a \in W(R)$ has the factorization $a = \prod_{m=1}^{\infty}(1-t^m)^{r_m}$ then it is seen that the nth ghost component is

$$gh_n(a) = \sum_{d|n} dr_d$$

A straightforward application of the Möbius inversion formula gives

Proposition 3 *Let $a \in W(R)$ where R is a binomial ring. Suppose*

$$gh(a) = g_1 t + g_2 t^2 + g_3 t^3 + \cdots$$

Then $a = \prod_{m=1}^{\infty}(1-t^m)^{r_m}$ where

$$r_m = \frac{1}{m}\sum_{d|m} \mu\left(\frac{m}{d}\right) g_d$$

where μ is the Möbius function.

2 The Grothendieck – Burnside ring

In this section I construct the Grothendieck – Burnside ring of [5] in the special case of the infinite cyclic group. In [5] this is constructed for any profinite group G, but I prefer to avoid all the technicalities involved. Thus let G denote the infinite cyclic group.

A (finite) G-space (S, σ) then consists simply of a finite set S together with a permutation σ of S. Thus G acts on S by $n \in G$ acting on $x \in S$ by $\sigma^n(x)$. Two G-spaces $(S, \sigma), (T, \tau)$ are isomorphic if there is a bijection $u : S \to T$ with $\tau u = u\sigma$. If $(S, \sigma), (T, \tau)$ are two G-spaces then there is a join $(S \bigsqcup T, \sigma \sqcup \tau)$ given by $S \bigsqcup T$ being the the disjoint union of S and T and

$$\sigma \sqcup \tau(x) = \begin{cases} \sigma(x) & \text{if } x \in S \\ \tau(x) & \text{if } x \in T \end{cases}$$

There is also the cartesian product G-space $(S \times T, \sigma \times \tau)$ where, of course, $\sigma \times \tau(x, y) = (\sigma(x), \tau(y))$.

I now let Ω be the Grothendieck group of the class of these (finite) G-spaces, i.e. Ω is the free abelian group generated by isomorphism classes $[S,\sigma]$ of G-spaces modulo the relation $[S \bigsqcup T, \sigma \sqcup \tau] = [S,\sigma] + [T,\tau]$. It is easily seen that the cartesian product operation induces a product on Ω so that Ω is a commutative ring.

Once again we have a ghost map. Here we define $Gh : \Omega \rightarrow t\mathbf{Z}[[t]]$ by $Gh([S,\sigma] = \sum_{n=1}^{\infty} Gh_n([S,\sigma])$ where $Gh_n([S,\sigma])$ is the number of elements of S left fixed by the action of the subgroup of G generated by n, i.e the number of elements of S left fixed by the permutation σ^n. This is well defined on isomorphism classes and is easily seen to be compatible with the ring structure on Ω and so factors as a ring homomorphism $Gh : \Omega \rightarrow t\mathbf{Z}[[t]]$ where the latter ring is viewed as the infinite product of the previous section.

The point is that this ghost map factors through the ghost map of the previous section, i.e. there is a map $\psi : \Omega \rightarrow W(\mathbf{Z})$ so that the diagram commutes.

$$\begin{tikzcd}
 & W(R) \arrow[d, "gh"] \\
\Omega \arrow[ur, "\psi"] \arrow[dr, "Gh"'] & \\
 & t\mathbf{Z}[[t]]
\end{tikzcd}$$

To see this, I first consider the case when (S,σ) is a transitive G-space, i.e. σ has only one orbit, i.e. is a cycle. Suppose that S has m elements. It is easily seen that σ^n has fixed points only if $m|n$, i.e. σ^n is the identity, in which case σ^n has m fixed points. Thus

$$Gh([S,\sigma]) = mt^m + mt^{2m} + mt^{3m} + \cdots = gh(1-t^m)$$

But every permutation is the product of disjoint cycles so in Ω each class $[S,\sigma]$ is a sum of transitive G-spaces. It follows that if σ factors as a product of r_m cycles of length m for $m = 1,2,3,\ldots$ then ψ should be given by

$$\psi([S,\sigma]) = (1-t)^{r_1}(1-t^2)^{r_2}(1-t^3)^{r_3}\cdots$$

It is easily checked that this does in fact work. It should be noted that since we are working with finite G-spaces that this "sum" is in fact finite, i.e. $r_m = 0$ for large m.

As a consequence of the above description of ψ one obtains

Proposition 4 *Let (S,σ) be a finite G-space with $\psi([S,\sigma]) = \prod_{m=1}^{\infty}(1-t^m)^{r_m}$. Then the number of distinct orbits of elements of S of length n under the permutation σ is r_n and the total number of distinct orbits is $\sum_{m=1}^{\infty} r_m$.*

3 Necklaces

In this section I apply the preceding results to counting necklaces. It should be emphasized that all the results here are classical, but given the preceding discussion I can give a much simpler exposition.

By a necklace with n beads in c colors, I mean an arrangement of n objects (beads) of c different colors around a circle. If the circle is rotated the resulting necklace is considered to be the same as the original, however a flip may produce a different necklace.

A more formal way of describing this is the following: let B be a set of n objects (the beads) and C be a set of c elements (the colors). Then consider the set S of the c^n functions $f : B \to C$. Now let γ be a cyclic permutation of the set S, i.e. there is only one orbit and γ has order n. Then there is a permutation σ of S given by $\sigma(f) = f \circ \gamma$. A necklace is an orbit in S of the permutation σ.

Thus (S, σ) is a G-space, so by Proposition 4 to count necklaces we need only calculate $\psi([S,\sigma])$. But since $gh : W(\mathbf{Z}) \to t\mathbf{Z}[[t]]$ is an injection, we can first calculate $Gh([S,\sigma])$ and lift.

Now the main observation is that f is a fixed point of σ^k if and only if f is constant on each orbit of γ^k. If k is relatively prime to n then γ^k again has only one orbit so f must be constant, i.e. $Gh_k([S,\sigma]) = c$. More generally, if $(k,n) = d$, (here and below (k,n) is the greatest common divisor) then γ^k has d orbits, on each of which f must be constant. Thus $Gh_k([S,\sigma]) = c^d$.

Example 5 Suppose I wish to know the number of necklaces with 6 beads of 5 possible colors. By the above paragraph

$$Gh([S,\sigma]) = 5t + 25t^2 + 125t^3 + 25t^4 + 5t^5 + 15625t^6 + \cdots$$

and is periodic of period 6. Using the technique of Example 2 (note even that the first 3 terms are the same) I easily calculate

$$\psi([S,\sigma)] = (1-t)^5(1-t^2)^{10}(1-t^3)^{40}(1-t^6)^{2580}$$

It follows from Proposition 4 that there are $5 + 10 + 40 + 2580 = 2635$ such necklaces.

Generalizing from the above example I note that by Proposition 4 of the last section, since the order of each cycle of σ divides n, that $\psi([S,\sigma]) = \prod_{d|n}(1-t^d)^{r_d}$. But $gh(1-t^d) = dt^d + dt^{2d} + \cdots + \frac{n}{d}t^n + \cdots$ so if we add the coefficients of t^i for $1 \le i \le n$ we get $\frac{n}{d}d = n$. Hence the coefficients of t^i, $1 \le i \le n$ in the expansion of $gh((1-t^d)^{r_d})$ add to nr_d and hence the coefficients of t^i, $1 \le i \le n$ of $Gh([S,\sigma]) = gh(\psi([S,\sigma])$ add to $n\left(\sum_{d|n} r_d\right)$. By Proposition 4 the sum in parentheses is the number of necklaces, and so one may conclude that the number of necklaces with n beads in c colors is

$$\frac{1}{n}\sum_{k=1}^{n} Gh_k([S,\sigma]) = \frac{1}{n}\sum_{k=1}^{n} c^{(k,n)}$$

But note that the number of times the term c^d appears in the last sum is $\phi(\frac{n}{d})$ where ϕ is Euler's ϕ function. And thus we obtain the classical formula:

Theorem 6 *The number of necklaces with n beads and c colors is*

$$\frac{1}{n}\sum_{d|n}\phi\left(\frac{n}{d}\right)c^d$$

I now look at the problem of counting primitive necklaces with n beads in c colors, let $M(c,n)$ denote the number of these. A primitive necklace is one which is asymmetric under rotation, i.e. corresponds to an orbit of length n in S under σ. Thus we see from Proposition 4 $M(c,n) = r_n$ where $\psi([S,\sigma]) = \prod_{m=1}^{\infty}(1-t^m)^{r_m}$. From this and Proposition 3 we immediately obtain the formula attributed to Col. Moreau

Theorem 7

$$M(c,n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)c^d$$

where μ is the Möbius function.

Motivated by Examples 2,5 the reader might observe that the "coefficient" r_n in the expansion $(1-ct) = \prod_{m=1}^{\infty}(1-r^m)^{r_m}$ is also given by the same formula $\sum_{d|n}\mu(\frac{n}{d})c^d$ and hence

$$(1-ct) = \prod_{n=1}^{\infty}(1-t^n)^{M(c,n)}$$

This identity usually occurs in the literature by replacing each side by its "negative" as

Theorem 8 (The Cyclotomic Identity) *For each positive integer c*

$$\frac{1}{1-ct} = \prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{M(c,n)}$$

Thus from Example 2 one may conclude that $M(5,1) = 5$, $M(5,2) = 10$, $M(5,3) = 40$, $M(5,4) = 150$, $M(5,5) = 624$ and $M(5,6) = 2580$ etc.

So far the multiplicative structure of $W(\mathbf{Z})$ has not played much of a role. As my last result, I derive an identity from [8] using Witt vector multiplication.

Theorem 9 *For integers i,j let (i,j) denote the greatest common divisor and $[i,j]$ be the least common multiple. Then for all positive integers a,b,n,*

$$M(ab,n) = \sum_{[i,j]=n}(i,j)M(a,i)M(b,j)$$

Proof: $M(ab,n)$ is the "coefficient" of $(1-t^n)$ in the expansion $(1-abt) = \prod_{m=1}^{\infty}(1-t^m)^{M(ab,m)}$ by the previous theorem. But in $W(\mathbf{Z})$, $(1-abt) = (1-at)*(1-bt)$ so

$$(1-abt) = \left(\prod_{i=1}^{\infty}(1-t^i)^{M(a,i)}\right) * \left(\prod_{j=1}^{\infty}(1-t^j)^{M(b,j)}\right)$$

By virtue of Equation 3 the $(1-t^n)$ term in this last product will be the "sum" of all products

$$(1-t^i)^{M(a,i)} * (1-t^j)^{M(b,j)} = (1-t^{[i,j]})^{(i,j)M(a,i)M(b,j)}$$

where $[i,j] = n$. This finishes the proof.

References

[1] G.M. Bergman, Ring Schemes, in “Lectures on Curves on an Algebraic Surface”(D. Mumford, ed.), Princeton Univ. Press, 1966.

[2] S. Bloch, Algebraic K-theory and Crystalline Cohomology, Publ. Math. I.H.E.S. 47 (1978), 188–268.

[3] N. Bourbaki, Algèbra Commutative, Ch. 9, Masson, 1983.

[4] P. Cartier, Groups formels associés aux anneaux de Witt généralisés, C.R. Acad. Sci. Paris 265 (1967), 49-52.

[5] A.W.M. Dress and C. Siebeneicher, The Burnside Ring of Profinite Groups and the Witt Vector Construction, Advances in Math 70, (1988), 87–132.

[6] John Graham, Generalised Witt Vectors, Advances in Math 99 (1993), 248–263.

[7] S. Lang, Algebra, Addison-Wesley, 1965.

[8] N. Metropolis and G-C. Rota, Witt Vectors and the Algebra of Necklaces, Advances in Math 50 (1983), 95–125.