Enumeration in categories of finite algebras

A. Meush and R. Quackenbush
Department of Mathematics
University of Manitoba
Winnipeg, Manitoba

At first glance, category theory may seem singularly inappropriate for studying combinatorics. Morphisms are the essence of category theory, but combinatorics tends to focus on structures and their substructures. When the typical morphisms are just embeddings, why bother with category theory? But there are naturally occurring examples where morphisms are not always 1-1. For instance, if our structures are totally unstructured, just sets, then every map is a morphism; moreover, some of the most fundamental enumerative combinatorics deals with sets and set mappings. Thus, there may well be a useful role for category theory in combinatorics.

One way of using category theory, due to A. Meush, is intimately connected with the concept of a factorization of a category; consequently, this approach can involve considerable category theory. However, in this paper we will only be using the universal algebraic concepts of direct product and subdirect product. For a much more general theory we refer the reader to [2], which is the Ph. D. thesis of the first author, completed under the supervision of the second author.

Let K' be a class of finite algebras closed under finite products and subalgebras; let K be the skeletal category associated with K': the objects of K consist of one member of each isomorphism class of K' and the morphisms are all algebra homomorphisms. Let $\mathbb{Z}(K)$ be the free $\mathbb{Z}$-module with basis the objects of K; we will define two multiplications on $\mathbb{Z}(K)$.

Let $Ob(K) = \{A_i \mid i \in I\}$; for $i, j \in I$, let $A_{p(i,j)}$ be that member of Ob(K) isomorphic to the direct product of A_i and A_j, $A_i \times A_j$. For the first multiplication, let $A_i \circ A_j = A_{p(i,j)}$ and extend to $\mathbb{Z}(K)$ linearly. For the second, let r(i, j, k) be the number of subdirect

subalgebras of $A_i \times A_j$ (i.e. subalgebras of $A_i \times A_j$ whose first projection is onto A_i and whose second projection is onto A_j) which are isomorphic to A_k and define $A_i \bullet A_j = \Sigma\, r(i, j, k)A_k$; extend to $\mathbf{Z}(K)$ linearly. Note that $r(i, j, k)$ is always finite and for fixed i and j, $r(i, j, k)$ is non-zero for only finitely many k. Thus, $\bullet$ is well defined.

Theorem ([2]): *$\langle \mathbf{Z}(K); \circ \rangle$ and $\langle \mathbf{Z}(K); \bullet \rangle$ are isomorphic rings.*

Proof: For $i \in I$, define $t(A_i) = \Sigma\, t(i, j)A_j$ where $t(i, j)$ is the number of subalgebras of A_i isomorphic to A_j; let t be the linear extension to a $\mathbf{Z}$-module endomorphism of $\mathbf{Z}(K)$. This will be our isomorphism from $\langle \mathbf{Z}(K); \circ \rangle$ to $\langle \mathbf{Z}(K); \bullet \rangle$. To see that multiplication is preserved, notice that $t(p(i, j), k) = \Sigma\, t(i, m)t(j, n)r(m, n, k)$. Hence, $t(A_i \circ A_j) = t(A_i) \bullet t(A_j)$. To complete the proof, we need to show that t is invertible. Let us write $t = id + u$ where id is the identity map and $u(A_i) = \Sigma\, \{t(i, j)A_j \mid i \neq j\}$. We can define a partial order on I by $i \leq j$ iff $t(j, i) > 0$ (i.e. iff A_i can be embedded into A_j). Then $u(A_i) = \Sigma\, \{t(i, j)A_j \mid j < i\}$. Since every principal order ideal of $\langle I, \leq \rangle$ is finite, u is locally nilpotent: for each $w \in \mathbf{Z}(K)$ there is an n such that $u^n(w) = 0$. This means that the inverse of t is $t^{-1} = \Sigma\, (-1)^i u^i$ (the local nilpotence of u guarantees that the sum is always finite).

Let $\mathrm{Hom}(A_i, A_j)$ be the set of all homomorphisms from A_i to A_j and $\mathrm{Sur}(A_i, A_j)$ the set of all onto homomorphisms from A_i to A_j; define $d(i, j) = |\mathrm{Sur}(A_i, A_j)|$ and $c(i, j) = |\mathrm{Hom}(A_i, A_j)|$. Define $d_i : \mathbf{Z}(K) \to \mathbf{Z}$ by $d_i(A_j) = d(i, j)$ and define $c_i : \mathbf{Z}(K) \to \mathbf{Z}$ by $c_i(A_j) = c(i, j)$, with both extended linearly. Finally, define $d : \mathbf{Z}(K) \to \mathbf{Z}^I$ by $d = (d_i)_{i \in I}$ and $c : \mathbf{Z}(K) \to \mathbf{Z}^I$ by $c = (c_i)_{i \in I}$.

Theorem ([2]): *$c : \langle \mathbf{Z}(K); \circ \rangle \to \mathbf{Z}^I$ and $d : \langle \mathbf{Z}(K); \bullet \rangle \to \mathbf{Z}^I$ are ring embeddings such that $dt = c$ and $ct^{-1} = d$.*

The proof is fairly straightforward and is left as an exercise. That c is an embedding was first proved by L. Lovász in [1] where it is the basis for his results on cancellation of common direct factors in categories of finite structures. Using these two theorems, we can compute a number of combinatorial identities. Let us write $t^{-1}(A_i) = \sum w(i, j)A_j$. Then it is easy to prove the following:

(a)	r(i, j, k)	=	$\sum w(i, m)w(j, n)t(p(m, n), k)$.
(b)	t(p(i, j), k)	=	$\sum t(i, m)t(j, n)r(m, n, k)$.
(c)	c(i, j)	=	$\sum t(j, k)d(i, k)$.
(d)	d(i, j)	=	$\sum w(j, k)c(i, k)$.
(e)	c(r, i)c(r, j)	=	c(r, p(i, j)).
(f)	d(r, i)d(r, j)	=	$\sum r(i, j, k)d(r, k)$.

Notation: To indicate a specific category K, the numerical functions r, t, c, d, w will be subscripted with the letter K.

Example 1: Finite Sets. For $1 \leq i < \infty$, let A_i be an i-element set. Our category is S, the category with object set $\{A_i \mid 1 \leq i < \infty\}$ and with all mappings as morphisms. Thus, $p_S(i, j) = ij$; $c_S(i, j) = j^i$; $d_S(i, j) = j!S(i, j)$ where S(i,j) is the Stirling number of the second kind; $t_S(i, j) = (ij)$; $w_S(i,j) = (-1)^{i-j}\binom{i}{j}$. The numbers $r_S(i, j, k)$ do not seem to have a common expression; they can be interpreted as the number of $i \times j$ (0,1)-matrices with at least one 1 in each row and column and exactly k 1s occurring. The identities (a)-(f) become:

(S_a)	$r_S(i, j, k)$	$= \sum (-1)^{i+j-m-n}\binom{i}{m}\binom{j}{n}\binom{mn}{k}$.
(S_b)	$\binom{ij}{k}$	$= \sum \binom{i}{m}\binom{j}{n} r_S(m, n, k)$.
(S_c)	j^i	$= \sum \binom{j}{k} k!S(i, k)$.
(S_d)	$j!S(i, j)$	$= \sum (-1)^{j-k}\binom{j}{k} k^i$.
(S_e)	$i^r j^r$	$= (ij)^r$.

(S_f) $\quad i!j!S(r, i)S(r, j) = \Sigma\, r_S(i, j, k)k!S(r, k)$

$= \Sigma\, (-1)^{i+j-m-n} \binom{i}{m} \binom{j}{n} \binom{mn}{k} k!S(r, k).$

Notice that (S_e) is trivial, (S_b) obvious by counting (0,1)-matrices, (S_c) and (S_d) well known; (S_a) is the inverse of (S_b); (S_f) can be obtained by interpreting $c_S(i, j)$ and $r_S(i, j, k)$ in the combinatorial manner already mentioned.

Example 2: Finite Boolean Algebras. For $1 \leq i < \infty$, let $\mathbf{B}_i$ be a boolean algebra with i atoms. Our category, B, has $\{\mathbf{B}_i \mid 1 \leq i < \infty\}$ as its object set with morphisms being the boolean homomorphisms. As is well known, B is dual to the category S. Thus, $p_B(i, j) = i + j$; by duality, $c_B(i, j) = i^j$; $d_B(i, j) = j! \binom{i}{j}$; $t_B(i, j) = S(i, j)$; $w(i, j) = s(i, j)$, the Stirling number of the first kind; $r_B(i, j, k) = \binom{i}{i+j-k} \binom{j}{i+j-k} (i + j - k)!$ (by duality; combinatorially this is the number of maps from an (i + j)-set onto a k-set whose restrictions to the first i elements and to the last j elements of the (i +j)-set are 1-1). The identities (a)-(f) become:

(B_a) $\quad \binom{i}{i+j-k} \binom{j}{i+j-k} (i + j - k)! = \Sigma\, s(i, m)s(j, n)S(m+n, k).$

(B_b) $\quad S(i+j, k) = \Sigma\, S(i, m)S(j, n) \binom{m}{m+n-k} \binom{n}{m+n-k} (m + n - k)!.$

(B_c) $\quad i^j = \Sigma\, S(j, k)k!(i^k).$

(B_d) $\quad j! \binom{i}{j} = \Sigma\, s(j, k)i^k.$

(B_e) $\quad i^j i^j = i^{i+j}.$

(B_f) $\quad i!j! \binom{r}{i} \binom{r}{j} = \Sigma \binom{i}{i+j-k} \binom{j}{i+j-k} (i+j-k)!k! \binom{r}{k};$

or

$$\binom{r}{i}\binom{r}{j} = \Sigma \binom{k}{i} \binom{i}{k-j} \binom{r}{k}.$$

Notice that (B_e) is trivial, (B_c) and (B_d) are standard, (B_f) is well known; (B_a) and (B_b) seem rather obscure. However, if we take $j = 1$ in (B_b), then we get the basic recurrence relation for Stirling numbers of the second kind: $S(i+1, k) = S(i, k-1) + kS(i, k)$.

There is an important special case, namely when $k = i$. In this case, $r(i, j, i) = d(i, j)$. This follows from the fact that each onto homomorphism $\phi: A_i \to A_j$ can be represented as $\{(a, \phi(a)) \mid a \in A_i\}$ which is a subdirect product of A_i and A_j isomorphic to A_i, and conversely. Combining equations (a) and (d) we get:

(g) $$\sum_n w(j, n)c(i, n) = \sum_{m,n} w(j, n)w(i, m)t(p(m, n), i).$$

Because t and t^{-1} are inverses of each other, for any sequences $\{a_i\}_{i \in I}$ and $\{b_i\}_{i \in I}$ of real numbers, we have: $a_i = \sum t(i, j)b_j$ for all i if and only if $b_i = \sum w(i, j)a_j$ for all i. Applying this inversion to (g) we get:

(h) $$c(i, n) = \sum w(i, m)t(p(m, n), i).$$

For our categories S and B, we get:

(S_h) $$j^i = \sum (-1)^{i-m} \binom{i}{m} \binom{mj}{i}.$$

(B_h) $$i^j = \sum s(i, m)S(m+j, i).$$

Equation (B_h) is particularly appealing because of its simplicity. Yet it is at best obscure and perhaps previously unknown.

Let us return to the rings $\langle \mathbb{Z}(K); \circ \rangle$ and $\langle \mathbb{Z}(K); \bullet \rangle$. Clearly, $\langle \mathbb{Z}(K); \circ \rangle$ is generated by D(K), those $A_i \in K$ which are directly irreducible. In fact, if K has unique direct factorization, then $\langle \mathbb{Z}(K); \circ \rangle$ is freely generated by D(K). What about $\langle \mathbb{Z}(K); \bullet \rangle$? Since it is isomorphic to $\langle \mathbb{Z}(K); \circ \rangle$, the same is true, but with t(D(K)), the image of D(K) under t, as (free) generating set. It is natural to ask whether D(K) itself is a (free) generating set for $\langle \mathbb{Z}(K); \bullet \rangle$.

Lemma : *$\langle Z(K); \bullet \rangle$ is generated by D(K).*

Proof: Induct on $|A_n|$; it suffices to show that each reducible A_n is a polynomial in some finite subset D of D(K) with $|A_i| < |A_n|$ for each $A_i \in D$. For this, use the equation $A_{p(i,j)} = A_i \bullet A_j - \Sigma \{r(i, j, k)A_k \mid k < p(i, j)\}$ and note that if $k < p(i, j)$, then $|A_k| < |A_{p(i,j)}|$.

Theorem ([2]): *If K has unique direct factorization, then D(K) is a free generating set for <Z(K); •>.*

Proof: For $i, j \in I$, define A_i *precedes* A_j if (A_i, A_j) is in the transitive closure of the union of the relations (i) that A_s is properly embeddable in A_t and (ii) that A_s is a proper direct factor of A_t. Note that if A_i precedes A_j, then $|A_i| < |A_j|$; thus, this relation is a partial order on I. The assumption that K has unique direct factorization implies that every finitely generated order ideal of I under this partial order is finite (if our type is finite, then we do not need unique factorization at this point). Let C be a finite subset of D(K) and D the members of D(K) belonging to the order ideal of I generated by C. It is easily seen that the subring of <Z(K); •> generated by D is the same as the subring of <Z(K); •> generated by $t(D) = \{t(A_i) \mid A_i \in D\}$; denote this ring by <Z(D); •>. But as t(D(K)) generates <Z(K ; •> freely, t(D) generates <Z(D); •> freely. Hence there is an onto endomorphism ϕ_D of <Z(D); •> defined by $\phi_D(t(A_i)) = A_i$ for all $A_i \in D$. But <Z(D); •>, being finitely generated, is Noetherian, and in a Noetherian ring every onto endomorphism is an isomorphism. Hence, if we define ϕ on <Z(K); •> by $\phi(t(A_i)) = A_i$ for all $A_i \in D(K)$, then ϕ extends to an isomorphism of <Z(K); •>, proving the theorem.

Corollary: *If K has unique direct factorization, then every A_i is expressible as a unique polynomial (with integer coefficients and zero constant term) in the members of D(K) which precede or equal A_i.*

Recall our embedding $d:\langle \mathbb{Z}(K), \bullet \rangle \rightarrow Z^I$. For each $n \in I$, $d(A_n)$ is the function $d(\_, n):I \rightarrow Z$ where $d(\_, n)(i) = d(i, n)$. Thus, we see that for each $n \in I$, there is a unique polynomial, P_n, (with integer coefficients and zero constant term) in the directly irreducibles A_i which precede or equal A_n (say, $A_1, ..., A_k$) such that $d(\_, n) = P_n(d(\_, 1), ..., d(\_, k))$.

For S, A_n is directly irreducible iff n is prime and A_i precedes A_j iff $i < j$. Since $d_S(i, j) = j!S(i, j)$, we see that for each n there is a unique polynomial P_n (with rational coefficients and zero constant term) in the primes $\leq n$ (say $p_1, ..., p_k$) such that $S(\_, n) = P_n(S(\_, p_1), ..., S(\_, p_k))$. For example, $S(\_, 4) = (1/6)S(\_, 2)^2 - S(\_, 3) - (1/6)S(\_, 2)$. The existence of such a polynomial can be inferred from equation (S_d). For B, B_1 is the only directly irreducible. The reader can check that the corresponding polynomial is well known.

References

[1] L. Lovász, Operations with structures, Acta Math. Sci. Hungar. 18(1967), 321-328.

[2] A. Meush, Categorical combinatorics, Ph.D. Thesis, University of Manitoba, Winnipeg, 1980.