TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 330, Number 2, April 1992

FUNCTORS ON THE CATEGORY OF FINITE SETS

RANDALL DOUGHERTY

ABSTRACT. Given a covariant or contravariant functor from the category of finite sets to itself, one can define a function from natural numbers to natural numbers by seeing how the functor maps cardinalities. In this paper we answer the question: what numerical functions arise in this way from functors? The sufficiency of the conditions we give is shown by simple constructions of functors. In order to show the necessity, we analyze the way in which functions in the domain category act on members of objects in the range category, and define combinatorial objects describing this action; the permutation groups in the domain category act on these combinatorial objects, and the possible sizes of orbits under this action restrict the values of the numerical function. Most of the arguments are purely combinatorial, but one case is reduced to a statement about permutation groups which is proved by group-theoretic methods.

1. INTRODUCTION

Let $\mathcal{FS}$ be the category of finite sets (with functions as morphisms). If F is a covariant or contravariant functor from $\mathcal{FS}$ to $\mathcal{FS}$, then the cardinality of $F(A)$ depends only on that of A, since F maps bijections to bijections; hence, we can define a function $\alpha\colon \omega \to \omega$ by $\alpha(|A|) = |F(A)|$. What properties can be proved about α, given that it arises from some functor F in this way? Can we find a necessary and sufficient condition on α for such an F to exist?

This question was asked by Bergman [4] as a goal to reach in the study of the structure of functors from $\mathcal{FS}$ to $\mathcal{FS}$. Bergman carried out this study far enough to settle the question for contravariant functors as well as the case $\alpha(0) > 0$ of the question for covariant functors; the remaining case, however, presented additional difficulties. In this paper, using an independently developed approach, we will give complete characterizations for both covariant and contravariant functors. In order to do so, we develop results on the structure of such functors which will be useful in further study even if no numerical questions are involved.

We say that a function $\alpha\colon \omega \to \omega$ is *represented* (*corepresented*) by a covariant (contravariant) functor $F\colon \mathcal{FS} \to \mathcal{FS}$ iff $|F(A)| = \alpha(|A|)$ for all A. It is not hard to see that the set of (co)represented functions is closed under sums and products, since we can apply corresponding operations (disjoint unions and products) to the (co)representing functors. Similarly, composing two represented functions or two corepresented functions gives a represented

Received by the editors December 4, 1989 and, in revised form, May 11, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 18B05, 20B25.
Key words and phrases. Functors, finite sets.

function, while composing a represented function and a corepresented function (in either order) results in a corepresented function. Trivial examples show that constant functions are both represented and corepresented and the identity function is represented. We now give three less trivial examples of covariant functors from $\mathcal{FS}$ to $\mathcal{FS}$ which illustrate some of the features which can occur; the general constructions we give later will be based on these examples.

(1) Fix a natural number k. Let $F_1(A)$ be the set $[A]^k$ of all k-element subsets of A, together with a separate element z_A; if $f\colon A \to B$, let

$$F_1(f)(x) = \begin{cases} z_B & \text{if } x = z_A \text{ or } f \text{ is not one-to-one on } x, \\ f\text{``}\,x & \text{otherwise} \end{cases}$$

(where $f\text{``}\,x$ is the image of x under f).

(2) Let $F_2(A)$ be the set of all nonempty subsets of A; if $f\colon A \to B$, let $F_2(f)(x) = f\text{``}\,x$.

(3) Let $F_3(A)$ be the set of all odd-cardinality subsets of A; if $f\colon A \to B$, let $F_3(f)(x)$ be the set of all $b \in B$ which have an odd number of preimages in x under f.

These three functors represent the functions $1 + \binom{n}{k}$, $\sum_{i=1}^{n} \binom{n}{i}$, and $\sum_{i \le n,\ i \text{ odd}} \binom{n}{i}$, respectively. F_1 has a contravariant analogue which uses partitions into k nonempty sets instead of subsets of size k.

The definition of the collection of (co)represented functions involves the collection of all functors from $\mathcal{FS}$ to $\mathcal{FS}$, and this would seem to indicate that the collection could be quite complicated. The following proposition, which is proved at the end of this section, shows that, at least in one sense, this is not the case.

Proposition 1.1. *The set of* (*co*)*represented functions is closed in the space of functions from ω to ω* (*under the product topology with ω discrete*).

This implies that the collection of (co)represented functions can be characterized by a (possibly infinite) list of conditions, each involving only finitely many values of the function. However, Proposition 1.1 does not guarantee that this list can be given effectively. The search for explicit conditions led to the constructions in §§2–4 of this paper, which finally yielded the characterizations given in the following theorems. (Theorems 1.2′ and 1.3 show that the list of finitary conditions can indeed be given effectively.)

Let Δ be the forward difference operator (so $\Delta\alpha(n) = \alpha(n+1) - \alpha(n)$), and let Δ^k be the k-fold iteration of Δ; then $\Delta^k\alpha(n) = \sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}\alpha(n+i)$. Let $S_n^{(m)}$ and $\mathcal{S}_n^{(m)}$ denote the Stirling numbers of the first and second kinds, respectively. (Recall that $\mathcal{S}_n^{(m)}$ is the number of partitions of a set of size n into exactly m nonempty subsets, and that the numbers $S_m^{(n)}$ are the coefficients in the inversion formula for the numbers $\mathcal{S}_m^{(n)}$ [1, Chapter 24].) Also, define the predicate $\Phi(M, N, k', k)$ to mean that M can be expressed as a sum of zero or more (not necessarily distinct) binomial coefficients $\binom{N}{i}$, where $1 \le i \le N$ and either $i < k'$ or i is an odd number less than k. (This makes sense even if k or k' is ω rather than a natural number.) If $\gamma\colon \omega \to \omega$ and $k, k' \le \omega$, define $\overline{\Phi}(\gamma, k', k)$ to mean that $\Phi(\gamma(N), N, k', k)$ holds for all natural numbers $N > k'$.

Theorem 1.2. *The function $\alpha\colon \omega \to \omega$ is represented by a covariant functor from $\mathscr{FS}$ to $\mathscr{FS}$ if and only if at least one of the following holds*:

(1) *There is a positive integer $r \le \alpha(1)$ such that, if we define $\beta\colon \omega \to \omega$ by $\beta(0) = r$ and $\beta(n) = \alpha(n)$ for $n > 0$, then $\Delta^k \beta(0) \ge 0$ for all $k \ge 0$.*

(2) *$\alpha(0) = 0$ and, if we define $\gamma(k)$ to be $\Delta^k \alpha(0)$, then $\gamma(k) \ge 0$ for all k; furthermore, if we define k_0, k_0', and k_0'' to be respectively the least odd k such that $\gamma(k) = 0$, the least $k > 0$ such that $\gamma(k) = 0$, and the least odd $k > 1$ such that $\gamma(k) \le 1$ (each of these minima is defined to be ω if no corresponding k exists), then $\overline{\Phi}(\gamma, k_0', k_0)$ and either $\overline{\Phi}(\gamma, k_0', k_0')$ or $\overline{\Phi}(\gamma, k_0'', k_0)$.*

Theorem 1.3 (Bergman). *The function $\alpha\colon \omega \to \omega$ is corepresented by a contravariant functor from $\mathscr{FS}$ to $\mathscr{FS}$ if and only if the following both hold*:

(1) *If there is an n such that $\alpha(n) = 0$, then $\alpha(n) = 0$ for all $n > 0$.*

(2) *For all $n \ge 0$, $\sum_{m=0}^{n} S_n^{(m)} \alpha(m) \ge 0$.*

Easy arguments show that Theorem 1.2 is equivalent to

Theorem 1.2′. *The function $\alpha\colon \omega \to \omega$ is represented by a covariant functor from $\mathscr{FS}$ to $\mathscr{FS}$ if and only if at least one of the following holds*:

(1) *There is an integer m with $\alpha(0) - \alpha(1) \le m < \alpha(0)$ such that, for all $k \ge 0$, $\Delta^k \alpha(0) \ge (-1)^k m$.*

(2) *$\alpha(0) = 0$ and, if we define $\gamma(k)$ to be $\Delta^k \alpha(0)$, then $\gamma(k) \ge 0$ for all $k < \omega$ and the following hold for all k, k', and k'' (including $k = \omega$ if so specified)*:

(a) *If k is odd and $\gamma(k) = 0$, then $\overline{\Phi}(\gamma, k, k)$.*

(b) *If $0 < k' < k$, k' is even, $\gamma(k') = 0$, and either k is odd and $\gamma(k) = 0$ or $k = \omega$, then $\overline{\Phi}(\gamma, k', k)$.*

(c) *If $1 < k'' < k' < k$, k'' is odd, $\gamma(k'') = 1$, k' is even, $\gamma(k') = 0$, and either k is odd and $\gamma(k) = 0$ or $k = \omega$, then either $\overline{\Phi}(\gamma, k', k')$ or $\overline{\Phi}(\gamma, k'', k)$.*

(The r in 1.2(1) and the m in 1.2′(1) are definable from each other by the equation $m + r = \alpha(0)$; it is now easy to see that 1.2(1) and 1.2′(1) are equivalent. As for the second parts, one just has to note that $\overline{\Phi}(\gamma, k', k)$ implies $\overline{\Phi}(\gamma, j', j)$ if $j' \ge k'$ and $j \ge k$ and then consider the cases $k_0' = k_0$ or $k_0' < k_0$ separately, with the latter case being divided into subcases $k_0'' \ge k_0'$ and $k_0'' < k_0'$, to see that 1.2(2) is equivalent to 1.2′(2).)

Under the standard inversion formulas, the conclusions of these theorems correspond to statements that α is expressible as a (possibly infinite) sum of certain basis functions. For the covariant version, define $\gamma(k)$ to be $\Delta^k \beta(0)$ in case (1). Then, in either case, we have $\gamma(m) \ge 0$, and $\alpha(n) = \sum_{m=0}^{n} \binom{n}{m} \gamma(m)$ for all $n > 0$. So, except at 0, α can be expressed as a sum of functions $n \mapsto \binom{n}{m}$ with coefficients $\gamma(m)$. The values $\gamma(m)$ can be chosen arbitrarily if $\gamma(0) > 0$ (case (1)); if $\gamma(0) = 0$, some extra conditions are imposed (case (2)). For the contravariant version, if we let $\gamma(n) = \sum_{m=0}^{n} S_n^{(m)} \alpha(m) \ge 0$, then $\alpha(n) = \sum_{m=0}^{n} \mathscr{S}_n^{(m)} \gamma(m)$, so α is the sum of functions $n \mapsto \mathscr{S}_n^{(m)}$ with coefficients $\gamma(m)$; these coefficients are arbitrary as long as $\gamma(0)$ and $\gamma(1)$ are positive (but otherwise $\gamma(n)$ must be 0 for all $n > 0$).

In §2 we will show the meaning of the numbers $\gamma(m)$ in terms of the structure of the (co)representing functor. For covariant functors, if α is given such that

$\gamma(0) > 0$, we will be able to put together functors like F_1 above to form a functor representing α. Similarly, for contravariant functors, if α leads to γ with $\gamma(0) > 0$ and $\gamma(1) > 0$, we can use the contravariant analogue of F_1 (which corepresents $1 + \mathscr{S}_n^{(k)}$) to get a functor which corepresents α.

For covariant functors, if $\gamma(0) = 0$, we use constructions based on F_2 and F_3; these constructions are given in §4. Roughly, the reason for the restrictions in (2) of Theorem 1.2$'$ is that $\gamma(k) = 0$ forces both F_2 and F_3 to be truncated at k, $\gamma(k') = 0$ forces F_2 to be truncated at k', and $\gamma(k'') = 1$ forces either F_2 or F_3 to be truncated at k''. The alternate functors we have to use once F_2 or F_3 is truncated represent functions with $\gamma(N) = \binom{N}{i}$ for some N and i.

The proofs in §§2–4 are purely combinatorial; in one case, however (the case $k' = 2$ of condition 1.2$'$(2)(b)), combinatorial arguments alone do not suffice, because the existence of certain strange permutation groups would allow us to construct functors representing functions violating this condition. Therefore, we must prove that such permutation groups do not exist; this proof is given in §5.

An interesting consequence of these two theorems is

Proposition 1.4. (1) *If α is a represented function, then either $\alpha(n)$ is a polynomial function of n for $n > 0$ or $\limsup_{n\to\infty} \sqrt[n]{\alpha(n)} \geq 2$ (so α, in a sense, grows at least exponentially).*

(2) *If α is a corepresented function, then either α is a finite sum of functions $n \mapsto \mathscr{S}_n^{(m)}$ (so $\alpha(n)$ is constant for $n > 0$ or grows exponentially) or*

$$\limsup_{n\to\infty} (\ln \alpha(n))/(n \ln n) \geq 1$$

(so, in a sense, α grows as n^n or $n!$ does, at least).

Proof. In both (1) and (2) we must show that, if $\gamma(m) > 0$ for infinitely many m, then the respective $\limsup$ is large. For (1), if $\gamma(m) > 0$, then $\alpha(2m) \geq \binom{2m}{m}$; since $\lim_{m\to\infty} \sqrt[2m]{\binom{2m}{m}} = 2$ by Stirling's formula, we get the desired result. For (2), we apply the easy estimate $\mathscr{S}_{m+n}^{(m)} \geq m^n$ with $n \sim m \ln m$; if $\gamma(m) > 0$, then $\alpha(m+n) \geq m^n$, and $\lim_{m\to\infty} (\ln m^n)/((m+n)\ln(m+n)) = 1$ for the above choice of n, so we are done. Q.E.D.

The $\limsup$ in the above is important; by making the m's where $\gamma(m) > 0$ sufficiently sparse, we can make the corresponding $\liminf$ 1 in (1) or 0 in (2). The explicit lower bound of 2 for the $\limsup$ in (1) means that many natural functions which grow exponentially (e.g., the Fibonacci sequence) are nonetheless not representable.

Some minor notational matters: We will treat the natural numbers as finite ordinals (i.e., each natural number is equal to the set of its predecessors). Let $[A]^n$ denote the set of all subsets of A of cardinality n. A partition of a set A is a collection of disjoint nonempty sets with union A; let $\operatorname{Part}(A, n)$ denote the set of partitions of A into n sets. The notations $f``X$ and $f^{-1}``X$ stand for the image and inverse image of the set X under the function f.

Proof of Proposition 1.1. Let $\mathscr{F}\mathscr{O}$ be the full subcategory of $\mathscr{F}\mathscr{S}$ whose objects are the finite ordinals (natural numbers); for $n \in \omega$, let $\mathscr{F}\mathscr{O}_n$ be the full subcategory of $\mathscr{F}\mathscr{O}$ with objects $0, 1, \ldots, n-1$. We can define the notion of a numerical function being (co)represented by a functor from $\mathscr{F}\mathscr{O}$ to $\mathscr{F}\mathscr{O}$ just as we did for $\mathcal{FS}$. We will show that any function which is a limit of functions (co)represented by functors from $\mathcal{FS}$ to $\mathcal{FS}$ is itself (co)represented by a functor from $\mathcal{FO}$ to $\mathcal{FO}$, and that any function which is (co)represented by a functor from $\mathcal{FO}$ to $\mathcal{FO}$ is (co)represented by a functor from $\mathcal{FS}$ to $\mathcal{FS}$.

Suppose $\alpha\colon \omega \to \omega$ is a limit of functions (co)represented by functors from $\mathcal{FS}$ to $\mathcal{FS}$. Let T be the set of covariant (contravariant) functors G from some $\mathcal{FO}_n$ to $\mathcal{FO}$ such that $G(m) = \alpha(m)$ for all $m < n$. Then T has a natural tree ordering (G_2 extends G_1 in the tree iff G_2 extends G_1 as a functor), and every level of the tree is finite (given the mapping on the objects of $\mathcal{FO}_n$, there are only finitely many ways to define the mapping on the morphisms). We now show that every level of T is nonempty. Given $n \in \omega$, there is a function $\beta\colon \omega \to \omega$ such that $\beta\restriction n = \alpha\restriction n$ and β is (co)represented by a functor $F\colon \mathcal{FS} \to \mathcal{FS}$. For each $m < n$, fix a bijection $h_m\colon F(m) \to \alpha(m)$. Then we can define a functor $G\colon \mathcal{FO}_n \to \mathcal{FO}$ by letting $G(m) = \alpha(m)$ and $G(f) = h_k \circ F(f) \circ h_m^{-1}$ for $f\colon m \to k$; G is on level n of T.

By the König Infinity Lemma, T has an infinite branch; the union of the functors along this branch is a functor $G\colon \mathcal{FO} \to \mathcal{FO}$ which (co)represents α.

Now suppose $G\colon \mathcal{FO} \to \mathcal{FO}$ (co)represents α. Then one could simply use the fact that $\mathcal{FO}$ is a skeleton of $\mathcal{FS}$ [10, §IV.4] to get a functor from $\mathcal{FS}$ to $\mathcal{FS}$ (co)representing α, by composing G with a retraction from $\mathcal{FS}$ to $\mathcal{FO}$; however, it requires the axiom of choice (on a proper class or on a subuniverse) to get such a retraction, and one can define a more natural (co)representing functor $F\colon \mathcal{FS} \to \mathcal{FS}$ directly as follows. First, assume G is covariant. For a finite set B, define $F(B)$ to be the set of all functions g such that:

(1) the domain of g is the set of all bijections from B to $|B|$;
(2) $g(h) \in G(|B|)$ for all h;
(3) if $h\colon B \to |B|$ and $s\colon |B| \to |B|$ are bijections, then $g(s \circ h) = G(s)(g(h))$.

Clearly we can define $g(h)$ arbitrarily for one such h, and then the third condition gives a unique definition of $g(h')$ for all other h', so $|F(B)| = |G(|B|)| = \alpha(|B|)$. Now, if $f\colon B \to C$, we define $F(f)$ by letting $F(f)(g)(h) = G(h \circ f \circ h'^{-1})(g(h'))$ for any $g \in F(B)$ and any bijections $h\colon C \to |C|$, $h'\colon B \to |B|$. This does not depend on the choice of h' since any other bijection from B to $|B|$ will be of the form $s \circ h'$ for some bijection $s\colon |B| \to |B|$, and (3) then ensures that we get the same value for $F(f)(g)(h)$. It is now easy to verify that F is a functor which represents α.

The contravariant case is similar; just replace $g(s \circ h) = G(s)(g(h))$ with $g(s \circ h) = G(s^{-1})(g(h))$. Q.E.D.

2. Control sets or partitions

In this section and the next one, when we are talking about a single fixed (covariant or contravariant) functor F, we will often write $\widehat{A}$ and $\hat{f}$ instead of $F(A)$ and $F(f)$. For now, fix a covariant functor $F\colon \mathcal{FS} \to \mathcal{FS}$.

Definition 2.1. If B is a finite set, $A \subseteq B$, and $x \in \widehat{B}$, then x is *controlled* by A iff, for any C and any $p, q\colon B \to C$, $p\restriction A = q\restriction A$ implies $\hat{p}(x) = \hat{q}(x)$.

Clearly every $x \in \widehat{B}$ is controlled by B. Note that, if $x \in \widehat{B}$ is controlled by A and $f\colon B \to C$, then $\hat{f}(x)$ is controlled by $f``A$: if $p, q\colon C \to D$ agree on $f``A$, then $p \circ f$ and $q \circ f$ agree on A, so $\hat{p}(\hat{f}(x)) = F(p \circ f)(x) = F(q \circ f)(x) = \hat{q}(\hat{f}(x))$.

Lemma 2.2. *If i is the inclusion map from A to B, and $x \in \hat{i}``\widehat{A}$, then $x$ is controlled by $A$. Conversely, if $A \neq \varnothing$ and $x$ is controlled by $A$, then $x \in \hat{i}``\widehat{A}$.*

Proof. The first part follows from what we just noted. Now suppose that x is controlled by A and $A \neq \varnothing$. Let $h\colon B \to A$ be a retraction (i.e., $h(x) = x$ for $x \in A$). Then $i \circ h$ and the identity map id_B agree on A, so $x = F(\mathrm{id}_B)(x) = F(i \circ h)(x) = \hat{i}\hat{h}(x)) \in \hat{i}``A$. Q.E.D.

Lemma 2.3. *If $x \in \widehat{B}$ is controlled by A and by A', then it is controlled by $A \cap A'$.*

Proof. Suppose x is controlled by A and by A', and $p, q\colon B \to C$ agree on $A \cap A'$. Define $r\colon B \to C$ so that $r(y)$ is $p(y)$ if $y \in A$, $q(y)$ otherwise. Then r agrees with p on A and with q on $(B \backslash A) \cup (A \cap A') \supseteq A'$, so $p(x) = r(x) = q(x)$. Therefore, x is controlled by $A \cap A'$. Q.E.D.

It follows that, for any $x \in \widehat{B}$, there is a least subset of B by which x is controlled, namely $\bigcap\{A \subseteq B\colon x \text{ is controlled by } A\}$; call this set B_x.

Lemma 2.4. *If $f\colon B \to C$ is one-to-one on B_x, then $C_{\hat{f}(x)} = f``B_x$.*

Proof. Let $A = B_x$. If $A = \varnothing$, then $\hat{f}(x)$ is controlled by $f``A = \varnothing$, so $C_{\hat{f}(x)} = \varnothing = f``A$; hence, we may assume $A \neq \varnothing$. Let $i\colon A \to B$ be the inclusion map, and let $g\colon f``A \to A$ be the inverse of $f \restriction A$. Let $\pi$ be a retraction from $C$ to $f``A$; then id_B and $i \circ g \circ \pi \circ f$ agree on A, so $\hat{i}(\hat{g}(\hat{\pi}(\hat{f}(x)))) = x$. Let A' be a proper subset of $f``A$; it will suffice to show that $\hat{f}(x)$ is not controlled by $A'$. Since $A' \subset f``A$, $g``A' \subset A = B_x$, so there are maps $p, q\colon B \to D$ which agree on $g``A'$ such that $\hat{p}(x) \neq \hat{q}(x)$. Then $p \circ i \circ g \circ \pi$ and $q \circ i \circ g \circ \pi$ agree on A' but $F(p \circ i \circ g \circ \pi)(\hat{f}(x)) = \hat{p}(x) \neq \hat{q}(x) = F(q \circ i \circ g \circ \pi)(\hat{f}(x))$, so $\hat{f}(x)$ is not controlled by A'. Q.E.D.

Lemma 2.5. *There is a function $\gamma\colon \omega \to \omega$ such that, for any finite $A \subseteq B$ with B nonempty, $|\{x \in \widehat{B}\colon B_x = A\}| = \gamma(|A|)$.*

Proof. It will suffice to prove that, if $A \subseteq B$, $A' \subseteq B'$, $B \neq \varnothing \neq B'$, and $|A| = |A'|$, then $|\{x \in \widehat{B}\colon B_x = A\}| = |\{x \in \widehat{B}'\colon B'_x = A'\}|$. Choose $f\colon B \to B'$ and $g\colon B' \to B$ such that $f \restriction A$ is a one-to-one mapping from A onto A' and $g \restriction A' = (f \restriction A)^{-1}$. By Lemma 2.4, $\hat{f}$ and $\hat{g}$ map the sets $\{x \in \widehat{B}\colon B_x = A\}$ and $\{x \in \widehat{B}'\colon B'_x = A'\}$ into each other. Since $g \circ f$ agrees with id_B on A, $\hat{g} \circ \hat{f}$ agrees with $\mathrm{id}_{\widehat{B}}$ on $\{x \in \widehat{B}\colon B_x = A\}$, so $\hat{f}$ is one-to-one on this set. Similarly, $\hat{g}$ is one-to-one on $\{x \in \widehat{B}'\colon B'_x = A'\}$. Therefore, $|\{x \in \widehat{B}\colon B_x = A\}| = |\{x \in \widehat{B}'\colon B'_x = A'\}|$. Q.E.D.

We say that the function γ is *realized* by the functor F.

Lemma 2.6. *If $\alpha\colon \omega \to \omega$ is represented by F and $\gamma\colon \omega \to \omega$ is realized by F, then $\alpha(n) = \sum_{m=0}^{\infty} \binom{n}{m} \gamma(m)$ for $n > 0$. If $\gamma(0) = 0$, then $\alpha(0) = 0$; if $\gamma(0) > 0$, then $\alpha(0)$ can be any natural number (i.e., if we change the value of*

$\alpha(0)$, *the resulting function will also be represented by some functor that realizes* γ).

Proof. If $B \neq \varnothing$, then

$$\alpha(|B|) = |\widehat{B}| = \sum_{A \subseteq B} |\{x \in \widehat{B} \colon B_x = A\}| = \sum_{A \subseteq B} \gamma(|A|)$$
$$= \sum_{k=0}^{\infty} \sum_{\substack{A \subseteq B \\ |A|=k}} \gamma(k) = \sum_{k=0}^{\infty} |[B]^k| \gamma(k) = \sum_{k=0}^{\infty} \binom{|B|}{k} \gamma(k).$$

If $x \in \widehat{\varnothing}$ and $i \colon \varnothing \to B$ is the inclusion map, then $\hat{i}(x)$ is controlled by i " $\varnothing = \varnothing$; therefore, $\alpha(0) \neq 0$ implies $\gamma(0) \neq 0$. Now, suppose $\gamma(0) \neq 0$, and suppose that $\beta \colon \omega \to \omega$ agrees with α everywhere except possibly at 0; we will construct a functor $G \colon \mathscr{FS} \to \mathscr{FS}$ which represents β and realizes γ. Let $G(B) = F(B)$ if $B \neq \varnothing$, and let $G(f) = F(f)$ if $f \colon B \to C$ and $B \neq \varnothing$; this ensures that G realizes γ and that $|G(B)| = \beta(|B|)$ for $B \neq \varnothing$. Let $G(\varnothing)$ be any set of size $\beta(0)$. To define $G(f)$ for $f \colon \varnothing \to C$, fix an element z of $F(\{1\})$ which is controlled by $\varnothing$ (this exists because $\gamma(0) \neq 0$), and let $G(f)(x) = g(z)$ for any $x \in G(\varnothing)$, where $g \colon \{1\} \to C$. Since z is controlled by $\varnothing$, $G(f)$ does not depend on the choice of g; since $g \colon \{1\} \to C$ and $h \colon C \to D$ give $h \circ g \colon \{1\} \to D$, G respects composition. Therefore, G is a functor representing β. Q.E.D.

Lemma 2.7. *If* $\gamma \colon \omega \to \omega$ *and* $\gamma(0) > 0$, *then* γ *is realized by some covariant functor* F.

Proof. Define the functor F as follows: for any B, let

$$F(B) = \bigcup_{m=0}^{\infty} ([B]^m \times \gamma(m))$$

and, for any $f \colon B \to C$ and any $(W, i) \in F(B)$, let

$$F(f)((W, i)) = \begin{cases} (f\text{“}\, W, i) & \text{if } f \text{ is one-to-one on } W, \\ (\varnothing, 0) & \text{otherwise.} \end{cases}$$

It is easy to see that F is a functor and that $B_{(W,i)} = W$, so F realizes γ. Q.E.D.

It should be noted that many (if not most) functors are much more complicated than the one constructed in this proof; the proof just gives a simple functor which suffices for the desired existence result. The same note applies to the other existence results we will prove.

If a function $\alpha \colon \omega \to \omega$ is represented by a functor F, then F realizes some function γ; the two cases in Theorem 1.2 correspond to the two possibilities $\gamma(0) > 0$ and $\gamma(0) = 0$. If $\gamma(0) > 0$ and we define $\beta(n)$ to be $\gamma(0)$ if $n = 0$ and $\alpha(n)$ if $n > 0$, then $\beta(n) = \sum_{m=0}^{\infty} \binom{n}{m} \gamma(m)$ for all n, so the standard inversion formula gives $\gamma(k) = \Delta^k \beta(0)$ and (1) of Theorem 1.2 holds. On the other hand, if $\gamma(0) = 0$, then we must have $\alpha(0) = 0$, so $\Delta^k \alpha(0) = \gamma(k) \geq 0$ for all k. The proof that the rest of (2) of Theorem 1.2 holds in this case requires more work and is given in §4.

Conversely, if $\alpha\colon \omega \to \omega$ satisfies (1) of Theorem 1.2, then $\gamma(k) = \Delta^k\beta(0) \geq 0$ for all k and $\gamma(0) > 0$, so γ is realized by some functor; then $\gamma(0) > 0$ and $\alpha(n) = \beta(n) = \sum_{m=0}^{\infty}\binom{n}{m}\gamma(m)$ for $n > 0$, so Lemma 2.6 implies that α is represented by some functor. If α satisfies 1.2(2), then we will see in §4 that the function γ defined by $\gamma(k) = \Delta^k\alpha(0)$ is realized by a functor F such that $F(\varnothing) = \varnothing$, so F represents α.

In the case of a contravariant functor $F\colon \mathscr{FS} \to \mathscr{FS}$, most of the preceding lemmas and proofs go through in a dual form which closely resembles the original. The results are stated below, but the only proofs given are those which differ from the preceding proofs by more than simple arrow reversals. Again, if we are talking about a fixed functor F, we will use $\widehat{B}$ and $\hat{f}$ to denote $F(B)$ and $F(f)$.

Definition 2.8. If B is a finite set, P is a partition of B, and $x \in \widehat{B}$, then x is *controlled* by P iff, for any $p, q\colon C \to B$, if p and q agree modulo P (i.e., p^{-1} " $W = q^{-1}$ " W for all $W \in P$), then $\hat{p}(x) = \hat{q}(x)$.

Clearly every $x \in \widehat{B}$ is controlled by the finest partition $\{\{b\}\colon b \in B\}$. If $x \in \widehat{B}$ is controlled by P and $f\colon C \to B$, then $\hat{f}(x)$ is controlled by the partition $P_f = \{f^{-1}$ " $W\colon W \in P\}\backslash\{\varnothing\}$.

Lemma 2.9. *If P is a partition of B and $e\colon B \to P$ is the canonical projection (i.e., $b \in e(b)$ for all $b \in B$), then $x \in \widehat{B}$ is controlled by P iff $x \in \hat{e}$ " $\widehat{P}$.*

Note that there is no exceptional case here, since for any partition P of any finite set B we can find a function $h\colon P \to B$ such that $h(W) \in W$ for all $W \in P$.

Lemma 2.10. *If $x \in \widehat{B}$ is controlled by P and by P', then it is controlled by the finest partition P'' coarser than both P and P'.*

(" P'' is coarser than P " means that every member of P is included in some member of P''. Note that we are using the term 'coarser' inclusively; that is, P is coarser than P.)

Proof. Two members a and b of B are in the same member of P'' iff there is a sequence $a = a_0, a_1, \dots, a_n = b$ for some (and hence for any sufficiently large) n such that a_{2k} and a_{2k+1} are in the same member of P and a_{2k+1} and a_{2k+2} are in the same member of P'. It follows that, if $p, q\colon C \to B$ agree modulo P'', then there is a sequence $p = p_0, p_1, \dots, p_n = q$ such that p_{2k} and p_{2k+1} agree modulo P while p_{2k+1} and p_{2k+2} agree modulo P'; this gives $\hat{p}(x) = \hat{p}_0(x) = \hat{p}_1(x) = \cdots = \hat{p}_n(x) = \hat{q}(x)$. Therefore, x is controlled by P''. Q.E.D.

Hence, for any $x \in \widehat{B}$, there is a coarsest partition B^x of B by which x is controlled.

Lemma 2.11. *If the range of $f\colon C \to B$ meets every member of $P = B^x$, then $C^{\hat{f}(x)} = P_f$.*

Lemma 2.12. *There is a function $\gamma\colon \omega \to \omega$ such that, for any partition P of a finite set B, $|\{x \in \widehat{B}\colon B^x = P\}| = \gamma(|P|)$.*

We say that the function γ is *corealized* by the contravariant functor F.

Lemma 2.13. *If $\alpha\colon \omega \to \omega$ is corepresented by F and $\gamma\colon \omega \to \omega$ is corealized by F, then $\alpha(n) = \sum_{m=0}^{\infty} \mathcal{S}_n^{(m)} \gamma(m)$ for $n \geq 0$.*

Proposition 2.14. *The function $\gamma\colon \omega \to \omega$ is corealized by some contravariant functor F iff either $\gamma(0) > 0$ and $\gamma(1) > 0$ or $\gamma(n) = 0$ for all $n > 0$.*

Proof. First suppose F corealizes γ. If B and C are finite sets with $B \neq \varnothing$, then there is a function $f\colon C \to B$, so there is a function $F(f)\colon F(B) \to F(C)$; hence, $\gamma(|B|) > 0$ implies $F(B) \neq \varnothing$, which implies $F(C) \neq \varnothing$. If $|C|$ is 0 or 1, then the only way to have $F(C) \neq \varnothing$ is to have $\gamma(|C|) > 0$. Hence, $\gamma(n) > 0$ for some $n > 0$ implies $\gamma(0) > 0$ and $\gamma(1) > 0$.

Next, suppose $\gamma(0) > 0$ and $\gamma(1) > 0$. Define the functor F as follows: for any B, let

$$F(B) = \bigcup_{m=0}^{\infty} (\mathrm{Part}(B, m) \times \gamma(m))$$

and, for any $f\colon C \to B$ and any $(P, i) \in F(B)$, let

$$F(f)((P, i)) = \begin{cases} (P_f, i) & \text{if } f\text{“ } C \text{ meets all elements of } P, \\ (\{C\}\backslash\{\varnothing\}, 0) & \text{otherwise.} \end{cases}$$

We easily verify that F is a contravariant functor and that $B^{(P,i)} = P$, so F corealizes γ.

Finally, if $\gamma(n) = 0$ for all $n > 0$, then γ is corealized by the contravariant functor F defined by: $F(B) = \varnothing$ for $B \neq \varnothing$, $F(\varnothing)$ is any set of size $\gamma(0)$, $F(\mathrm{id}_\varnothing) = \mathrm{id}_{F(\varnothing)}$, and $F(f)$ is the unique function from $\varnothing$ to $F(C)$ whenever $f\colon C \to B$, $B \neq \varnothing$. Q.E.D.

If the function $\alpha\colon \omega \to \omega$ is corepresented by the functor F, then F corealizes some function $\gamma\colon \omega \to \omega$. Applying the standard inversion formula to Lemma 2.13 gives $\sum_{m=0}^{\infty} S_n^{(m)} \alpha(m) = \gamma(n)$, and in particular $\alpha(0) = \gamma(0)$ and $\alpha(1) = \gamma(1)$. It is now easy to prove Theorem 1.3 from Proposition 2.14.

The reason that the contravariant case is simpler than the covariant case for this problem seems to be that a trivial partition has size 1, while a trivial subset has size 0. If there are elements controlled by trivial sets or partitions, then we are free to add elements which behave nontrivially at only one place; this is the proof of Lemma 2.7 and Proposition 2.14. If there are no such elements, then in the contravariant case only $F(\varnothing)$ can be nonempty, so we can easily list all of the possibilities; in the covariant case, $F(\varnothing) = \varnothing$, but the rest of the functor could be quite complicated.

3. Control structures

Let $F\colon \mathcal{FS} \to \mathcal{FS}$ be a fixed covariant functor. For any finite set B and any $x \in \widehat{B}$, we have defined B_x to be the smallest set by which x is controlled. If $f\colon B \to C$ is one-to-one on B_x, then $C_{\hat{f}(x)} = f\text{“ } B_x$ by Lemma 2.4; if f is not one-to-one on B_x, however, we cannot determine $C_{\hat{f}(x)}$ from B_x in many cases (as will be clear from examples to follow). We now define a structure which will encode the value of $C_{\hat{f}(x)}$ for all such C and f.

Recall from §2 that, if $f\colon B \to C$ and P is a partition of C, then we get an induced partition $P_f = \{f^{-1}\text{“ } W\colon W \in P\}\backslash\{\varnothing\}$ of B. Let e_{fP} be the canonical map from P_f to P (i.e., if $x \in W \in P_f$, then $f(x) \in e_{fP}(W)$).

Also, if P and Π are partitions of B and Π is coarser than P (i.e., each member of P is included in some member of Π), let $e_{P\Pi}$ be the canonical map from P to Π (i.e., $W \subseteq e_{P\Pi}(W)$ for each $W \in P$).

Definition 3.1. A *control structure* on a finite set B is a function h such that:

(1) the domain of h is the set of partitions of B;
(2) for each P, $h(P) \subseteq P$;
(3) if Π is coarser than P, then $h(\Pi) \subseteq e_{P\Pi}\text{“}\,h(P)$; and
(4) if Π is coarser than P and $e_{P\Pi}$ is one-to-one on $h(P)$, then $h(\Pi) = e_{P\Pi}\text{“}\,h(P)$.

Suppose $x \in \widehat{B}$. For any partition P of B, let $h(P) = P_{\hat{g}(x)}$, where g is the projection from B to P; then h will be a control structure on B, which we call the control structure of x and denote by $K_F(B)(x)$. The control structure of x is enough to tell us what $C_{\hat{f}(x)}$ is for any function f from B to C—the function f induces a partition P on B ($P = \Pi_f$, where $\Pi = \{\{c\} : c \in C\}$), there is a unique one-to-one function $f' : P \to C$ such that $f = f' \circ g$ with g as above, and $C_{\hat{f}(x)} = f'\text{“}\,h(P)$ by Lemma 2.4.

If $x \in \widehat{B}$, $f : B \to C$, and $f' : C \to D$, then $\hat{f}'(\hat{f}(x)) = \widehat{f'\circ f}(x)$; this indicates that we should be able to compute the control structure of $\hat{f}(x)$ from that of x. Given a control structure h on B and a function $f : B \to C$, define a function h' by letting $h'(P) = e_{fP}\text{“}\,h(P_f)$ for any partition P of C. It is not hard to verify that h' is a control structure on C (when verifying (3) and (4), it is useful to note that, if Π is coarser than P, then $e_{P\Pi} \circ e_{fP} = e_{f\Pi} \circ e_{P_f\Pi_f}$), which we denote by $Q(f)(h)$.

The proof of the following proposition consists of straightforward verifications, so it is not written out here.

Proposition 3.2. (1) *If $Q(B)$ is the set of control structures on B, and $Q(f)$: $Q(B) \to Q(C)$ is defined as above for $f : B \to C$, then Q is a covariant functor from $\mathscr{FS}$ to $\mathscr{FS}$.*

(2) *If F is a covariant functor from $\mathscr{FS}$ to $\mathscr{FS}$, and $K_F(B) : F(B) \to Q(B)$ is defined as above, then K_F is a morphism of functors from F to Q.*

In the proof that Q is a functor, the only place where we used properties (3) and (4) of a control structure h was in proving the same properties for $Q(f)(h)$. That is, if we had omitted these properties from the definition, Proposition 3.2 would still hold; these are just extra properties that happened to be true of $K_F(B)(x)$ for any $x \in \widehat{B}$. One might ask whether there are further properties which could have been added to the definition of control structure; the following proposition answers this question negatively.

Proposition 3.3. *K_Q is the identity morphism from Q to Q.*

Proof. We must show that, for any finite set B and any $h \in Q(B)$, $K_Q(B)(h) = h$. Let P be any partition of B, and let g be the projection from B to P; then $K_Q(B)(h)(P) = P_{Q(g)(h)}$, so we must show that $P_{Q(g)(h)} = h(P)$.

Given $W \in h(P)$, choose a set D and one-to-one functions $p, q : P \to D$ which differ at W but nowhere else. Let $\Pi = \{\{d\} : d \in D\}$, and let $j(d) = \{d\}$ for $d \in D$. Then

$$Q(p)(Q(g)(h))(\Pi) = Q(p \circ g)(h)(\Pi) = e_{(p\circ g)\Pi}\text{“}\,h(\Pi_{p\circ g}).$$

But it is easy to see that $\Pi_{p \circ g} = P$ and $e_{(p \circ g)\Pi} = j \circ p$, so $Q(p)(Q(g)(h))(\Pi) = j \text{ “ } p \text{ “ } h(P)$. Similarly, $Q(q)(Q(g)(h))(\Pi) = j \text{ “ } q \text{ “ } h(P)$. Since j, p, and q are one-to-one and p and q differ only at W, $Q(p)(Q(g)(h))(\Pi) \neq Q(q)(Q(g)(h))(\Pi)$. But p and q agree on $P\backslash\{W\}$; therefore, $P_{Q(g)(h)} \not\subseteq P\backslash\{W\}$, so $W \in P_{Q(g)(h)}$. Since W was arbitrary, $h(P) \subseteq P_{Q(g)(h)}$.

Now suppose $p, q\colon P \to D$ agree on $h(P)$. Let Π be any partition of D. Let Π' be the coarsest common refinement of Π_p and Π_q; that is, $\Pi' = \{W \cap V\colon W \in \Pi_p,\ V \in \Pi_q\}\backslash\{\varnothing\}$. Also, let $\widetilde{P} = \{\{W\}\colon W \in P\}$ and let $j(W) = \{W\}$ for $W \in P$. The following diagram will be useful:

$$\begin{tikzcd}
B \arrow[r, "g"] & P \arrow[r, "e_{P\Pi'_g}"] \arrow[d, "j"] & \Pi'_g \arrow[r, "e_{\Pi'_g(\Pi_p)_g}"] \arrow[d, "e_{g\Pi'}"] & (\Pi_p)_g \arrow[d, "e_{g\Pi_p}"] & \\
 & \widetilde{P} \arrow[r, "e_{\tilde{P}\Pi'}"'] & \Pi' \arrow[r, "e_{\Pi'\Pi_p}"'] & \Pi_p \arrow[r, "e_{p\Pi}"'] & \Pi
\end{tikzcd}$$

Since Π'_g is coarser than $P = \widetilde{P}_g$, 3.1(3) gives $h(\Pi'_g) \subseteq e_{P\Pi'_g} \text{ “ } h(P)$, so $h(\Pi'_g) = e_{P\Pi'_g} \text{ “ } S$ for some $S \subseteq h(P)$. If W and V are elements of $h(P)$, then $e_{\widetilde{P}\Pi_p}(\{W\}) = e_{\widetilde{P}\Pi_p}(\{V\}) \Leftrightarrow p(W) = p(V)$, and the same holds for q; since p and q agree on $h(P)$,

$$\begin{aligned} e_{\widetilde{P}\Pi_p}(\{W\}) = e_{\widetilde{P}\Pi_p}(\{V\}) &\Leftrightarrow e_{\widetilde{P}\Pi_q}(\{W\}) = e_{\widetilde{P}\Pi_q}(\{V\}) \\ &\Leftrightarrow e_{\widetilde{P}\Pi'}(\{W\}) = e_{\widetilde{P}\Pi'}(\{V\}). \end{aligned}$$

Therefore, $e_{\Pi'\Pi_p}$ and $e_{\Pi'\Pi_q}$ are one-to-one on $e_{\widetilde{P}\Pi'} \text{ “ } j \text{ “ } h(P)$. We have $j = e_{g\widetilde{P}}$ and $\widetilde{P}_g = P$, so $e_{\widetilde{P}\Pi'} \circ j = e_{g\Pi'} \circ e_{P\Pi'_g}$. Hence, $e_{\Pi'\Pi_p}$ is one-to-one on $e_{g\Pi'} \text{ “ } e_{P\Pi'_g} \text{ “ } h(P) \supseteq e_{g\Pi'} \text{ “ } h(\Pi'_g)$. Since $e_{g\Pi'}$ is one-to-one, $e_{\Pi'\Pi_p} \circ e_{g\Pi'}$ is one-to-one on $h(\Pi'_g)$. We also have $e_{\Pi'\Pi_p} \circ e_{g\Pi'} = e_{g\Pi_p} \circ e_{\Pi'_g(\Pi_p)_g}$, so $e_{\Pi'_g(\Pi_p)_g}$ is one-to-one on $h(\Pi'_g)$. By 3.1(4), $h((\Pi_p)_g) = e_{\Pi'_g(\Pi_p)_g} \text{ “ } h(\Pi'_g)$. Therefore,

$$\begin{aligned} Q(p)(Q(g)(h))(\Pi) &= e_{p\Pi} \text{ “ } Q(g)(h)(\Pi_p) = e_{p\Pi} \text{ “ } e_{g\Pi_p} \text{ “ } h((\Pi_p)_g) \\ &= e_{p\Pi} \text{ “ } e_{g\Pi_p} \text{ “ } e_{\Pi'_g(\Pi_p)_g} \text{ “ } h(\Pi'_g) \\ &= e_{p\Pi} \text{ “ } e_{g\Pi_p} \text{ “ } e_{\Pi'_g(\Pi_p)_g} \text{ “ } e_{P\Pi'_g} \text{ “ } S \\ &= e_{p\Pi} \text{ “ } e_{g\Pi_p} \text{ “ } e_{\Pi'_g(\Pi_p)_g} \text{ “ } \{W \in \Pi'_g\colon (\exists V \in S)\ V \subseteq W\} \\ &= e_{p\Pi} \text{ “ } e_{g\Pi_p} \text{ “ } \{W \in (\Pi_p)_g\colon (\exists V \in S)\ V \subseteq W\} \\ &= e_{p\Pi} \text{ “ } \{W \in \Pi_p\colon (\exists V \in S)\ g \text{ “ } V \subseteq W\} \\ &= \{W \in \Pi\colon (\exists V \in S)\ p \text{ “ } g \text{ “ } V \subseteq W\} \\ &= \{W \in \Pi\colon (\exists V \in S)\ p(V) \in W\}. \end{aligned}$$

The same argument gives $Q(q)(Q(g)(h))(\Pi) = \{W \in \Pi\colon (\exists V \in S)\ q(V) \in W\}$. But p and q agree on $h(P) \supseteq S$, so $Q(p)(Q(g)(h))(\Pi) = Q(q)(Q(g)(h))(\Pi)$. Since Π was arbitrary, $Q(p)(Q(g)(h)) = Q(q)(Q(g)(h))$; since p and q were arbitrary, $Q(g)(h)$ is controlled by $h(P)$. Therefore, $P_{Q(g)(h)} = h(P)$, as desired. Q.E.D.

Since the value of $K_F(B)(x)$ depends only on the behavior of $F(f)(x)$ for maps $f\colon B \to C$, we have $K_G(B)(x) = K_F(B)(x)$ if G is a subfunctor of F

(i.e., $G(B) \subseteq F(B)$ for all B and $G(f) = F(f)\restriction G(B)$ for all $f\colon B \to C$) such that $x \in G(B)$. This will be useful in constructing examples; if x is a control structure on B, then the subfunctor G of Q generated by $x \in Q(B)$ will be relatively simple, but we will still have $K_G(B)(x) = x$.

We now describe the analogues of Q and K_F for contravariant functors. These are not needed for Theorem 1.3, of course, but they may be useful for further study of these functors.

Definition 3.4. A *dual control structure* on a finite set B is a function h such that:

(1) the domain of h is the set of subsets of B;
(2) if $A \subseteq B$, then $h(A)$ is a partition of A;
(3) if $A' \subseteq A \subseteq B$, and $i\colon A' \to A$ is the inclusion map, then $h(A')$ is coarser than $(h(A))_i$; and
(4) if $A' \subseteq A \subseteq B$ and A' meets all members of $h(A)$, then $h(A') = (h(A))_i$.

Suppose $x \in F(B)$. For any $A \subseteq B$, let $h(A) = A^{F(i)(x)}$, where i is the inclusion map from A to B; then h will be a dual control structure on B, which we call the dual control structure of x and denote by $K_F^d(B)(x)$. The dual control structure of x is enough to tell us what $C^{F(f)(x)}$ is for any $f\colon C \to B$: if $A = f\text{“}C$, then $C^{F(f)(x)} = (h(A))_f$.

Given a dual control structure h on B and a function $f\colon C \to B$, define a function h' by letting $h'(D) = (h(f\text{“}D))_{f\restriction D}$ for any $D \subseteq C$. Then h' is a dual control structure on C, which we denote by $Q^d(f)(h)$. Again it is straightforward to prove

Proposition 3.5. (1) *If $Q^d(B)$ is the set of dual control structures on B, and $Q^d(f)\colon Q^d(B) \to Q^d(C)$ is defined as above for $f\colon C \to B$, then Q^d is a contravariant functor from $\mathscr{FS}$ to $\mathscr{FS}$.*

(2) *If F is a contravariant functor from $\mathscr{FS}$ to $\mathscr{FS}$, and $K_F^d\colon F(B) \to Q^d(B)$ is defined as above, then K_F^d is a morphism of functors from F to Q^d.*

Proposition 3.6. *$K_{Q^d}^d$ is the identity morphism from Q^d to Q^d.*

Proof. We must show that, for any finite set B and any $h \in Q^d(B)$, $K_{Q^d}^d(B)(h) = h$. Let A be any subset of B, and let $i\colon A \to B$ be the inclusion map; then $K_{Q^d}^d(B)(h)(A) = A^{Q^d(i)(h)}$, so we must show that $A^{Q^d(i)(h)} = h(A)$.

First, suppose $h(A)$ is not coarser than $A^{Q^d(i)(h)}$. Choose $a, b \in A$ which are in the same member of $A^{Q^d(i)(h)}$ but not in the same member of $h(A)$. Let $C = A \cup \{c\}$ for some $c \notin A$, and define $p, q\colon C \to A$ to be the identity on A but send c to a and b, respectively. Then

$$Q^d(p)(Q^d(i)(h))(C) = Q^d(i \circ p)(h)(C) = (h((i \circ p)\text{“}C))_{(i\circ p)} = (h(A))_{(i\circ p)}$$

and $Q^d(q)(Q^d(i)(h))(C) = (h(A))_{(i\circ q)}$; these partitions differ, since c is in the same element as a in the former but not in the latter. But p and q agree modulo $A^{Q^d(i)(h)}$, so $Q^d(p)(Q^d(i)(h)) = Q^d(q)(Q^d(i)(h))$, a contradiction. Therefore, $h(A)$ is coarser than $A^{Q^d(i)(h)}$; it remains to show that $Q^d(i)(h)$ is controlled by $h(A)$.

Let C be a finite set, and suppose that $p, q\colon C \to A$ agree modulo $h(A)$. Let D be a subset of C, and let $D' = (p \text{ ``} D) \cup (q \text{ ``} D)$. By 3.4(3), $h(D')$ is coarser than $(h(A))_{i'}$, where i' is the inclusion from D' to A. Since p and q agree modulo $h(A)$, $p\restriction D$ and $q\restriction D$ agree modulo $h(A)$ and hence modulo $h(D')$. It follows that $p\text{``}D$ meets all elements of $h(D')$, so, by 3.4(4), $h(p \text{ ``} D) = (h(D'))_{i''}$, where $i''\colon p \text{ ``} D \to D'$ is the inclusion map. We now get

$$Q^d(p)(Q^d(i)(h))(D) = Q^d(i \circ p)(h)(D) = (h((i \circ p) \text{ ``} D))_{(i\circ p)\restriction D} = (h(D'))_{p\restriction D}.$$

The same argument gives $Q^d(q)(Q^d(i)(h))(D) = (h(D'))_{q\restriction D}$. But $p\restriction D$ and $q\restriction D$ agree modulo $h(D')$, so $Q^d(p)(Q^d(i)(h))(D) = Q^d(q)(Q^d(i)(h))(D)$. Since D, C, p and q were arbitrary, $Q^d(i)(h)$ is controlled by $h(A)$. Q.E.D.

4. Definable sets and minimal sets

In this section we will complete the proof of Theorems 1.2 and 1.2′ (except for one group-theoretic result whose proof is given in the next section). Because of the remarks following Lemma 2.7, this reduces to proving the following characterization of realizable functions:

Theorem 4.1. *A function $\gamma\colon \omega \to \omega$ is realized by some covariant functor if and only if either $\gamma(0) > 0$ or γ satisfies the conditions given for γ in* 1.2(2) (*or, equivalently,* 1.2′(2)).

The ‘if’ part will be proved by an explicit construction at the end of this section; for now we will work on the ‘only if’ part. Again consider a fixed covariant functor $F\colon \mathcal{FS} \to \mathcal{FS}$. The action of the symmetric group Sym(B) on a finite set B is mapped by F to an action of Sym(B) on $F(B)$; the function $K_F(B)\colon F(B) \to Q(B)$ preserves this group action. Therefore, the size of the orbit of $x \in F(B)$ under Sym(B) is a multiple of the size of the orbit of $h = K_F(B)(x)$. Note that the set $\{x \in F(B)\colon B_x = B\}$, which has cardinality $\gamma(|B|)$ if F realizes γ, is closed under the group action and hence is a union of orbits. In order to prove $\Phi(\gamma(|B|), |B|, k', k)$, it will suffice to show that any x in the above set lies in an orbit whose size is a multiple of $\binom{|B|}{m}$ for some $m > 0$ which is less than k and either odd or less than k'; this will follow if we can show that the orbit of the corresponding h has size divisible by $\binom{|B|}{m}$.

We say that a subset A of B is *definable from* $h \in Q(B)$ iff every member of Sym(B) which fixes h also fixes A. In this case, if $\mathrm{Sym}(B)_h$ and $\mathrm{Sym}(B)_{\{A\}}$ are the stabilizers of h and A, respectively, within Sym(B), then $|\mathrm{Sym}(B)_h|$ divides $|\mathrm{Sym}(B)_{\{A\}}|$, so the size of the orbit of h under Sym(B) (which is $n!/|\mathrm{Sym}(B)_h|$) is a multiple of the size of the orbit of A (which is $n!/|\mathrm{Sym}(B)_{\{A\}}| = \binom{|B|}{|A|}$).

Suppose $|B| > 1$ and h is a control structure on B such that $h(P) \neq \varnothing$ for all partitions P of B. A *minimal set* for h is defined to be a nonempty set $T \subset B$ such that $T \in h(\{T, B\backslash T\})$ but $T' \notin h(\{T', B\backslash T'\})$ for all nonempty $T' \subset T$. Since $h(P) \neq \varnothing$ for all P, minimal sets for h exist. Note that the union of all minimal sets for h is an example of a subset of B definable from h (it is easy to see that, if T is minimal for h and $s \in \mathrm{Sym}(B)$, then $s \text{ ``} T$ is minimal for $Q(s)(h)$); another example is the union of all minimal sets of cardinality greater than 1.

If h is as above and P is a partition of B, define $\mathrm{Odd}(h, P)$ to be the following assertion: for any partition Π coarser than P (recall that this includes the case $\Pi = P$), $h(\Pi) = \{W \in \Pi\colon |e_{P\Pi}^{-1}\text{“}\{W\}| \text{ is odd}\}$.

Now consider the following statements:

Statement (not Theorem) 4.2. *Suppose h is a control structure on B, $|B| > 1$, and $h(P) \neq \varnothing$ for all P. Let A be the union of all minimal sets for h of size greater than 1 if there are any; otherwise, let A be the union of all minimal sets for h.*

(1) *If $k > 1$ is odd, and $|h(P)| \neq k$ for all P, then $|A| < k$.*

(2) *If $k' > 1$, and $|h(P)| \neq k'$ for all P, then $|A|$ is either less than k' or odd.*

(3) *If $1 < k'' < k'$, k'' is odd, $|h(P)| \neq k'$ for all P, and there is no partition P of B such that $|P| = k''$ and $\mathrm{Odd}(h, P)$, then $|A| < k'$.*

(4) *If $k'' > 1$ is odd, and every partition P of B such that $|P| = k''$ and $h(P) = P$ satisfies $\mathrm{Odd}(h, P)$, then $|A|$ is either less than k'' or odd.*

These statements imply Theorem 4.1:

Proposition 4.3. *Suppose $\gamma\colon \omega \to \omega$ is realized by a covariant functor, and $\gamma(0) = 0$. If Statement 4.2 (1) is true (for all h), then γ must satisfy 1.2′(2)(a); if 4.2 (1) and 4.2 (2) are true, then γ must satisfy 1.2′(2)(b); if 4.2 (1), 4.2 (3), and 4.2 (4) are true, then γ must satisfy 1.2′(2)(c). In fact, if 4.2 (1) is true for a particular k, then γ must satisfy 1.2′(2)(a) for that k; corresponding statements hold for the other parts of 1.2′(2).*

Proof. Let F be a functor realizing γ. If $h = K_F(B)(x)$ for some $x \in F(B)$, then the set A from Statement 4.2 is clearly definable from h; by the remarks following the statement of Theorem 4.1, it will suffice to prove certain cardinality restrictions on A, since the size of the orbit of x will be a multiple of $\binom{|B|}{|A|}$.

For 1.2′(2)(a), the case $k = 1$ is trivial (if $\gamma(0) = \gamma(1) = 0$, then $F(1) = \varnothing$, so $F(B) = \varnothing$ for all B by applying F to some $f\colon B \to 1$), so assume k is an odd number greater than 1; it will suffice to show that $\gamma(k) = 0$ implies $|A| < k$. Since F realizes γ and $\gamma(k) = 0$, we have $|h(P)| \neq k$ for all partitions P of B. (For any such P, if $g\colon B \to P$ is the canonical projection, then $|P_{\hat{g}(x)}| = |h(P)|$, so $\gamma(|h(P)|) > 0$.) Hence, 4.2(1) gives $|A| < k$, as desired. Note that, as well as taking care of 1.2′(2)(a), this shows that $|A| < k$ for the remaining two parts of this proposition (this is obvious when $k = \omega$).

Part (b) of 1.2′(2) is just as easy. Assuming $1 < k' < k$, $\gamma(k') = 0$, and either k is odd and $\gamma(k) = 0$ or $k = \omega$, we must show that $|A|$ is less than k and either odd or less than k'; the former follows from the preceding paragraph and the latter follows from 4.2(2), since $\gamma(k') = 0$ gives $|h(P)| \neq k'$ for all P.

Now assume the hypotheses of 1.2′(2)(c). Let D be a fixed set of size k''; then $\gamma(k'') = 1$ implies that there is a unique element x_0 of $F(D)$ such that $D_{x_0} = D$. We now ask whether $\mathrm{Odd}(h_0, \tilde{D})$ holds, where $h_0 = K_F(D)(x_0)$ and $\tilde{D} = \{\{d\}\colon d \in D\}$. This is relevant because, for any h as above, if P is a partition of B such that $|P| = k''$ and $h(P) = P$, then $\mathrm{Odd}(h, P)$ holds if and only if $\mathrm{Odd}(h_0, \tilde{D})$ holds. (Since $|P| = |D|$, there is a function f mapping B onto D such that $\tilde{D}_f = P$. This and $h(P) = P$ imply $D_{\hat{f}(x)} = D$, so $\hat{f}(x)$

must be x_0. Hence, $Q(f)(h) = h_0$, and it follows immediately that $\mathrm{Odd}(h, P)$ is equivalent to $\mathrm{Odd}(h_0, \widetilde{D})$.)

If $\mathrm{Odd}(h_0, \widetilde{D})$ does not hold, then $\mathrm{Odd}(h, P)$ does not hold for any P such that $|P| = k''$. Now 4.2(3) implies that $|A| < k'$. Since h is arbitrary (but h_0 is fixed), we have $\Phi(\gamma(|B|), |B|, k', k')$ by the usual reasoning.

On the other hand, if $\mathrm{Odd}(h_0, \widetilde{D})$ does hold, then $\mathrm{Odd}(h, P)$ holds for all P such that $|P| = k''$ and $h(P) = P$. Now 4.2(1) gives $|A| < k$ as before, while 4.2(4) implies that $|A|$ is either less than k'' or odd. This is just what is needed to prove $\Phi(\gamma(|B|), |B|, k'', k)$, so we are done. Q.E.D.

The last remark in the statement of Proposition 4.3 is needed; it turns out that one subcase of Statement 4.2 is not true, and we will have to resort to other methods to prove the corresponding part of 1.2′(2). The rest of Statement 4.2 will be proved using the following six lemmas; throughout these lemmas, assume that h is a control structure on B, $|B| > 1$, and $h(P) \neq \varnothing$ for all P.

Lemma 4.4. (1) *If T is a minimal set for B and P is a partition of B such that $T \in P$, then $T \in h(P)$.*

(2) *If P_1 is a partition of a minimal set T for h into more than one subset, P_2 is a partition of B, and $P_1 \subset P_2$, then $P_1 \subset h(P_2)$ (strict inclusion).*

Proof. (1) Apply 3.1(3) to P and $\Pi = \{T, B\backslash T\}$.

(2) Suppose $U \in P_1$ and $U' = T\backslash U$. We know that the minimal set T is in $h(\{T, B\backslash T\})$, so by 3.1(3) at least one of U and U' is in $h(\{U, U', B\backslash T\})$. If $U \notin h(\{U, U', B\backslash T\})$, then $U' \in h(\{U, U', B\backslash T\})$, so 3.1(4) gives $U' \in h(\{U', B\backslash U'\})$, contradicting the minimality of T; therefore, $U \in h(\{U, U', B\backslash T\})$. Similarly, $U' \in h(\{U, U', B\backslash T\})$. We also have $B\backslash T \in h(\{U, U', B\backslash T\})$, since otherwise 3.1(4) would give $U' \in h(\{U', B\backslash U'\})$, again contradicting the minimality of T. Now 3.1(3) gives

$$U \in h(P_1 \cup \{B\backslash T\}) \quad \text{and} \quad B\backslash T \in h(P_1 \cup \{B\backslash T\});$$

since U was arbitrary, $h(P_1 \cup \{B\backslash T\}) = P_1 \cup \{B\backslash T\}$. One more application of 3.1(3) gives the desired result. Q.E.D.

Lemma 4.5. *If $|B| \geq k \geq 3$ and the union of all minimal sets for h of size greater than 1 has size at least k, then there is a partition P of B of size k such that $h(P) = P$ and some element of P is a proper subset of a minimal set.*

Proof. Let $S = \{T_1, T_2, \ldots, T_m\}$ be a collection of minimal sets for h, each of size greater than 1, such that $|\bigcup S| \geq k$ and m is as small as possible (so $|\bigcup(S\backslash\{T_i\})| < k$ for all $i \leq m$). If $m = 1$, then we can let P be $\{B\backslash T_1\}$ together with a partition of T_1 into $k-1$ pieces, and Lemma 4.4(2) will imply that $h(P) = P$; so assume $m > 1$. Let $b_1, b_2, \ldots, b_l$ be a list of the members of $\bigcup S$, arranged so that the b's not in T_m come first, followed by the b's occurring both in T_m and in some other T_i, and finally the b's in T_m only; in particular, we will have $b_1 \notin T_m$ and $T_i \subseteq \{b_1, b_2, \ldots, b_{k-1}\}$ for $i < m$.

Let $W = B\backslash\{b_1, b_2, \ldots, b_{k-1}\}$, and let $\Pi_1 = \{\{b_1\}, \ldots, \{b_{k-1}\}, W\}$. If $h(\Pi_1) = \Pi_1$, we are done, so assume this is not the case. In particular, this implies $B \neq \bigcup S$, since otherwise Lemma 4.4 would give $h(\Pi_1) = \Pi_1$. For any b_j which is in T_i for some $i < m$, we have $\{b_j\} \in h(\Pi_1)$ by Lemma 4.4(2); hence, either $W \notin h(\Pi_1)$ or $\{b_j\} \notin h(\Pi_1)$ for some b_j which is in T_m but in no other T_i. By rearranging the list $b_1, b_2, \dots, b_{k-1}$, we may ensure that either $W \notin h(\Pi_1)$ or $\{b_{k-1}\} \notin h(\Pi_1)$.

Now let

$$\Pi_2 = \{\{b_1\}, \dots, \{b_{k-2}\}, W \cup \{b_{k-1}\}\}$$

and

$$\Pi_3 = \{\{b_1\}, \dots, \{b_{k-2}\}, U, W'\},$$

where $U = T_m \backslash \{b_1, \dots, b_{k-2}\}$ and $W' = (B \backslash T_m) \backslash \{b_1, \dots, b_{k-2}\}$. If $j \leq k-2$ and $b_j \in T_i$ for some $i < m$, then $\{b_j\} \in h(\Pi_1)$ as noted above, so $\{b_j\} \in h(\Pi_2)$ by 3.1(4), so $\{b_j\} \in h(\Pi_3)$ by 3.1(3); if $j \leq k-2$ and $b_j \in T_m$, then $\{b_j\} \in h(\Pi_3)$ by Lemma 4.4(2). Lemma 4.4 also gives $U \in h(\Pi_3)$. If $W' \in h(\Pi_3)$, we are done, so assume $W' \notin h(\Pi_3)$.

Finally, let $\Pi_4 = \{\{b_2\}, \dots, \{b_{k-2}\}, U, W' \cup \{b_1\}\}$ and

$$\Pi_5 = \{\{b_2\}, \dots, \{b_{k-2}\}, U \backslash \{b_k\}, \{b_k\}, W' \cup \{b_1\}\}.$$

(Since $|T_m| > 1$, we have either $b_{k-1} \in U$ or $b_{k+1} \in U$, so $U \backslash \{b_k\}$ is nonempty.) Then $h(\Pi_4) = \Pi_4$ by 3.1(4), so all elements of Π_5 other than $U \backslash \{b_k\}$ and $\{b_k\}$ are in $h(\Pi_5)$ by 3.1(3). But $U \backslash \{b_k\}$ and $\{b_k\}$ are also in $h(\Pi_5)$ by Lemma 4.4(2), so we are done. Q.E.D.

Lemma 4.6. *Suppose that $n \geq 3$, and h has the following property: for any partition P of B, if $|P| = n$ and $h(P) = P$, then* Odd(h, P) *holds. Then the union of all minimal sets for h having size greater than 1 has size less than n.*

Proof. Suppose not; then Lemma 4.5 gives a partition P of B such that $|P| = n$, $h(P) = P$, and some $W \in P$ is a proper subset of a minimal set. Then the definition of minimality gives $W \notin h(\{W, B \backslash W\})$ while Odd(h, P) gives $W \in h(\{W, B \backslash W\})$, so we have a contradiction. Q.E.D.

Lemma 4.7. *Assume the hypotheses of Lemma 4.6, and also suppose that all minimal sets for h have size 1 and that there are at least n of them. Then the number of minimal sets for h is odd. Furthermore, one of the following two cases holds:*

(1) *For every partition P' of B of the form $\{\{b_1\}, \{b_2\}, \dots, \{b_{n-1}\}, W\}$ where the sets $\{b_i\}$ are distinct minimal sets, we have $h(P') = P'$. In this case, n must be odd.*

(2) *For every such partition P', we have $W \notin h(P')$. In this case, n is even, the hypothesis of 4.6 holds vacuously (i.e., there is no partition P of B such that $|P| = n$ and $h(P) = P$), and for any odd $n'' < n$ there is a partition P'' of B into n'' pieces such that* Odd(h, P'') *holds (and hence $h(P'') = P''$).*

Proof. Let $A = \{b \in B\colon \{b\} \text{ is minimal}\}$. Note that, for any $S \subset A$ of size $n-1$, the sets $\{b\}$ for $b \in S$ are all in $h(\{\{b\}\colon b \in S\} \cup \{B \backslash S\})$ by Lemma 4.4(1). Say that such a set S is of type (1) if $B \backslash S \in h(\{\{b\}\colon b \in S\} \cup \{B \backslash S\})$; otherwise, say that S is of type (2). The first step is to show that either all sets S are of type (1) (we abbreviate this by saying "case (1) holds") or all S are of type (2) ("case (2) holds").

Suppose this is not the case; say S is of type (1) and S' is of type (2). We can get from S to S' by a sequence of operations, each of which replaces a single member of the current set with an element of S'; one of these steps must move from a type (1) set to a type (2) set, so there exist a type (1) set and a type (2) set which differ only by one element. In other words, there exist a set $W \subset A$ of size $n-2$ and elements b', b'' of $A \backslash W$ such that $W \cup \{b'\}$ is of type (1) but $W \cup \{b''\}$ is of type (2). But then the hypothesis of 4.6 gives $B \backslash W \notin h(\{\{b\}: b \in W\} \cup \{B \backslash W\})$, while Definition 3.1(4) gives $B \backslash W \in h(\{\{b\}: b \in W\} \cup \{B \backslash W\})$, so we have a contradiction. Therefore, either case (1) or case (2) holds.

Let $b_1, b_2, \ldots, b_l$ be a list of the members of A, where $l = |A|$. None of what follows will depend on which particular listing is chosen, so if we prove a fact about a partition defined from one such listing, the same fact will hold about the corresponding partition defined from another listing. The main partitions we will be working with are:

$$P_m = \{L_m, \{b_{m+1}\}, \{b_{m+2}\}, \ldots, \{b_{m+n-2}\}, R_{m+n-1}\},$$
$$P'_m = \{L_m, \{b_{m+1}\}, \{b_{m+2}\}, \ldots, \{b_{m+n-3}\}, R_{m+n-2}\},$$

where $L_m = \{b_1, b_2, \ldots, b_m\}$ and $R_m = B \backslash L_{m-1}$. This definition for P_m is valid if $m+n-2 \le \min(l, |B|-1)$, and the definition for P'_m is valid if $m+n-3 \le \min(l, |B|-1)$. Note that all of the members of P_m other than L_m and R_{m+n-1} must be in $h(P_m)$ by Lemma 4.4(1); the same holds for P'_m.

For now, suppose case (1) holds; then $h(P_1) = P_1$ and, because $\mathrm{Odd}(h, P_1)$ holds, $h(P'_1) = P'_1 \backslash \{R_{n-1}\}$. Clearly n must be odd, since otherwise $\mathrm{Odd}(h, P_1)$ would give $h(\{B\}) = \varnothing$. We now show by induction on m that $h(P_m)$ is P_m if m is odd, $P_m \backslash \{L_m, R_{m+n-1}\}$ if m is even, while $h(P'_m)$ is $P'_m \backslash \{R_{m+n-2}\}$ if m is odd, $P'_m \backslash \{L_m\}$ if m is even. If $h(P'_m) = P'_m \backslash \{R_{m+n-2}\}$, then $L_m \in h(P_m)$ by 3.1(3), and $R_{m+n-1} \in h(P_m)$ since otherwise 3.1(4) would give $R_{m+n-2} \in h(P'_m)$, so $h(P_m) = P_m$; now $\mathrm{Odd}(h, P_m)$ gives $h(P'_{m+1}) = P'_{m+1} \backslash \{L_{m+1}\}$. On the other hand, if $h(P'_m) = P'_m \backslash \{L_m\}$, then we cannot have both of L_m and R_{m+n-1} in $h(P_m)$ because this would imply $\mathrm{Odd}(h, P_m)$ and hence $L_m \in h(P'_m)$, and we cannot have exactly one of them in $h(P_m)$ because then 3.1(4) would give $h(\widehat{P}) = \widehat{P}$, where

$$\widehat{P} = \{\{b_{m+1}\}, \{b_{m+2}\}, \ldots, \{b_{m+n-2}\}, B \backslash \{b_{m+1}, \ldots, b_{m+n-2}\}\},$$

and this cannot happen for the same reason that it could not happen for P'_1 ($\widehat{P}$ is just like P_1 except for a rearrangement of the listing of A). Therefore, $h(P_m) = P_m \backslash \{L_m, R_{m+n-1}\}$, and now 3.1(4) gives $h(P'_{m+1}) = P'_{m+1} \backslash \{R_{m+n-1}\}$. This completes the induction.

If $|A| = l$ is even and $A = B$, then $R_l = \{b_l\}$ is in $h(P_{l-n+1})$ by Lemma 4.4(1), but the above gives $R_l \notin h(P_{l-n+1})$, a contradiction. If l is even and $A \neq B$, then the above results give $h(P_{l-n+2}) = P_{l-n+2}$, so we get $\mathrm{Odd}(h, P_{l-n+2})$ and hence $R_{l+1} \in h(\{R_{l+1}, B \backslash R_{l+1}\})$, so some subset of R_{l+1} is a minimal set. But $R_{l+1} = B \backslash A$ and A is the union of all minimal sets for h (of size 1, but there are none of size greater than 1), so this is also impossible. Therefore, l must be odd. This completes the proof of the lemma in case (1).

From now on, assume that case (2) holds; this gives $h(P_1) = P_1 \backslash \{R_n\}$ and, by 3.1(4), $h(P'_1) = P'_1$. Note that $|B|$ must be greater than n, since otherwise R_n would be $\{b_n\}$ and would be in $h(P_1)$ by Lemma 4.4(1). We now show by induction on m that $h(P_m)$ is $P_m \backslash \{R_{m+n-1}\}$ if m is odd, $P_m \backslash \{L_m\}$ if m is even, while $h(P'_m)$ is P'_m if m is odd, and $R_{m+n-2} \notin h(P'_m)$ if m is even. If $h(P'_m) = P'_m$, then $L_m \in h(P_m)$ by 3.1(3), and $h(P_m)$ cannot be P_m since otherwise we would have $\mathrm{Odd}(h, P_m)$ and hence $R_{m+n-2} \notin h(P'_m)$, so we must have $h(P_m) = P_m \backslash \{R_{m+n-1}\}$; now 3.1(3) gives $R_{m+n-1} \notin h(P'_{m+1})$. On the other hand, suppose $R_{m+n-2} \notin h(P'_m)$. Then R_{m+n-1} must be in $h(P_m)$, since otherwise 3.1(4) would give $R_{m+n-2} \in h(P'_m)$. Also, we cannot have $L_m \in h(P_m)$, since otherwise $\mathrm{Odd}(h, P_m)$ would give $h(\widehat{P}) \neq \widehat{P}$, where $\widehat{P}$ is defined as in the previous case; this is impossible because $\widehat{P}$ is just like P'_1 except for a rearrangement of the listing of A. Therefore, $h(P_m) = P_m \backslash \{L_m\}$, so $h(P'_{m+1}) = P'_{m+1}$ by 3.1(4). This completes the induction.

Claim. If $U \subseteq V \subseteq A$, $|U| = 2$, $|V| \leq n$, and P is a partition of B such that U and $B \backslash V$ are in P, then $U \notin h(P)$.

Proof. We may choose the listing $b_1, b_2, \ldots, b_l$ of A so that $U = \{b_1, b_2\}$ and $V \subseteq L_n$. Since $|B| > n$, P_2 is defined, and the above results give $U \notin h(P_2)$. But P is coarser than P_2, so 3.1(3) gives $U \notin h(P)$. Q.E.D.

We now show that, for any partition Π of B such that $R_n \in \Pi$, we have $h(\Pi) = \{U \in \Pi\colon U \neq R_n \text{ and } |U| \text{ is odd}\}$. Create a new partition P of B by breaking up each $U \in \Pi$ other than R_n into pieces of size 2, together with one piece of size 1 if $|U|$ is odd. Then 3.1(3) applied to P_1 and P gives $R_n \notin h(P)$, the Claim implies that no set of size 2 is in $h(P)$, and Lemma 4.4(1) forces all of the leftover pieces of size 1 to be in $h(P)$, so $h(P)$ is the set of these leftover pieces of size 1. Now 3.1(4) applied to P and Π shows that $h(\Pi)$ is as stated.

It follows immediately that n must be even, since otherwise $h(\{L_{n-1}, R_n\})$ would be empty. Since n is even, the hypothesis of 4.6 can only hold vacuously; if there were a partition P with $|P| = n$ and $h(P) = P$, then $\mathrm{Odd}(h, P)$ would give $h(\{B\}) = \varnothing$.

Next, suppose n'' is an odd number less than n, and define P'' to be $\{\{b_1\}, \ldots, \{b_{n''-1}\}, R_{n''}\}$; the property we need to show for P'' is equivalent to the statement that, for any Π coarser than P'', $h(\Pi) = \{U \in \Pi\colon |U \cap L_{n''}| \text{ is odd}\}$, since each element of P'' contains exactly one element of $L_{n''}$. Given such a Π, let U be the element of Π including $R_{n''}$, and create a new partition Π' from Π by breaking U up into $U \cap L_{n-1}$ and R_n. Then $W \in \Pi'$ is in $h(\Pi')$ if and only if $W \neq R_n$ and $|W|$ is odd. But the elements $b_{n''+1}, b_{n''+2}, \ldots, b_{n-1}$ are in the same element of Π', and there are evenly many of them, so they cancel each other out; that is, W is in Π' iff $W \cap L_{n''}$ is odd. Now 3.1(4) implies the same result for Π, as desired.

It remains to show that $l = |A|$ is odd. If l is even and $A = B$, then we get $R_l \notin h(P_{l-n+1})$ since $l - n + 1$ is odd; but this is impossible, since Lemma 4.4(1) gives $R_l = \{b_l\} \in h(P_{l-n+1})$. Finally, suppose that l is even but less than $|B|$. Let

$$S = \{\{b_{l-n+3}, b_{l-n+4}\}, \{b_{l-n+5}, b_{l-n+6}\}, \ldots, \{b_{l-1}, b_l\}\}.$$

Then 3.1(3) applied to P_{l-n+2} gives $L_{l-n+2} \notin h(S \cup \{L_{l-n+2}, R_{l+1}\})$. Also, no member of S can be in $h(S \cup \{L_{l-n+2}, R_{l+1}\})$, since otherwise 3.1(4) would imply that this same member is in $h(S \cup \{L_{l-n+2} \cup R_{l+1}\})$, contradicting the Claim. Therefore, 3.1(3) gives $L_l \notin h(\{L_l, R_{l+1}\})$, so $R_{l+1} \in h(\{L_l, R_{l+1}\})$, so some subset of R_{l+1} is a minimal set. But, as before, this is impossible because $R_{l+1} = B\backslash A$ and A is the union of all minimal sets. This completes the proof of Lemma 4.7. Q.E.D.

Lemma 4.8. *If k is an odd number such that $|h(P)| \neq k$ for all P, and all minimal sets for h have size 1, then there are fewer than k minimal sets for h.*

Proof. Suppose not; then $k > 1$ since $h(\{B\}) = \{B\}$, so the hypotheses of Lemma 4.7 are satisfied for $n = k$ (the hypothesis of 4.6 holds vacuously). Since n is odd, it must be case (1) of the conclusion that holds; but then any P' as in this conclusion satisfies $|h(P')| = |P'| = k$, a contradiction. Q.E.D.

Lemma 4.9. *If k is an odd number such that $|h(P)| \neq k$ for all P, and $|B| \geq k$, then there is a set $C \subseteq B$ definable from h such that $|C| < k$ and either $|C|$ is odd or $h(\{\{a\}: a \in C\} \cup \{B\backslash C\}) = \{\{a\}: a \in C\}$.*

Proof. Proceed by induction on k (which, as noted in the preceding lemma, must be at least 3). Let A be the union of all minimal sets for h of size greater than 1, if there are any; otherwise, let A be the union of all minimal sets for h. Then A is nonempty and definable from h, and Lemmas 4.5 and 4.8 imply that $|A| < k$; also, by Lemma 4.4, $\{\{a\}: a \in A\} \subseteq h(\{\{a\}: a \in A\} \cup P)$ for any partition P of $B\backslash A$. If $|A|$ is odd, or if $B\backslash A \notin h(\{\{a\}: a \in A\} \cup \{B\backslash A\})$, then we can just let $C = A$. Otherwise, let $\overline{B} = B\backslash A$ and $\overline{k} = k - |A|$, and define $\overline{h} \in Q(\overline{B})$ by $\overline{h}(P) = h(\{\{a\}: a \in A\} \cup P) \cap P$. Then $|\overline{h}(P)| \neq \overline{k}$ for all P. Apply the induction hypothesis to get a set $\overline{C} \subseteq \overline{B}$ definable from $\overline{h}$ such that $|\overline{C}| < \overline{k}$ and either $|\overline{C}|$ is odd or $\overline{h}(\{\{a\}: a \in \overline{C}\} \cup \{\overline{B}\backslash\overline{C}\}) = \{\{a\}: a \in \overline{C}\}$; then let $C = \overline{C} \cup A$. Q.E.D.

Proposition 4.10. *Parts (1), (3), and (4) of Statement 4.2 are true for all k, k', and k''; and part (2) is true for all k and all $k' > 2$.*

Proof. Let B, h, and A be as in Statement 4.2.

If $k > 1$ is odd and $|h(P)| \neq k$ for all P, then Lemma 4.5 gives $|A| < k$ if there is a minimal set of size greater than 1, while Lemma 4.8 gives $|A| < k$ if all minimal sets have size 1; this proves 4.2(1).

Now consider the case $k' > 2$ of 4.2(2). If there is a minimal set for h of size greater than 1, then $|A| < k'$ by Lemma 4.5; if not, then either $|A| < k'$ or $|A|$ is odd by Lemma 4.7 with $n = k'$ (the hypothesis of 4.6 holds vacuously). Therefore, $|A|$ is as required.

If the hypotheses of 4.2(3) hold, then the conclusion of Lemma 4.7 fails for $n = k'$, so one of the hypotheses must fail; but the hypotheses of 4.6 hold vacuously (there is no P such that $|P| = n$ and $h(P) = P$), so either there is a minimal set for h of size greater than 1 (in which case Lemma 4.5 gives $|A| < k'$) or all minimal sets have size 1 but there are fewer than n of them (which gives $|A| < k'$ immediately). So $|A| < k'$ in any case.

Finally, assume the hypotheses of 4.2(4). If there is a minimal set for h of size greater than 1, then $|A| < k''$ by Lemma 4.6 with $n = k''$; if all minimal sets for h have size 1, then $|A|$ is either less than k'' or odd by Lemma 4.7 with $n = k''$. Q.E.D.

This suffices to prove all of Theorem 4.1 except for the case $k' = 2$ of 1.2′(2)(b). Unfortunately, the remaining part of Statement 4.2 is not true; in fact, there are control structures h such that $|h(P)|$ is never 0 or 2 but no set of odd cardinality is definable from h. To see this, we will construct a control structure h on the set $B = \{1, 2, 3, 4, 5, 6\}$. For any partition P of B, let $h(P) = P$ if $|P| \neq 2$. If $|P| = 2$, say $P = \{U, V\}$, then look at the pairs $\{1, 2\}$, $\{3, 4\}$, and $\{5, 6\}$, in that order; if any one of these pairs is included in U or in V, then let W be the one of U and V which includes the first such pair, and let $h(P) = \{W\}$. Otherwise, let W be that one of U and V which contains zero or two members of $\{1, 3, 5\}$, and again let $h(P) = \{W\}$. It is easy to show that h is a control structure on B, and $|h(P)| \neq 2$ for all partitions P of B. But h is fixed under the subgroup

$$\{\mathrm{id}_B, (1\ 2)(3\ 4), (1\ 2)(5\ 6), (3\ 4)(5\ 6)\}$$

of $\mathrm{Sym}(B)$, which fixes no subset of B of odd cardinality (because such a subset must split one of the pairs $\{1, 2\}$, $\{3, 4\}$, or $\{5, 6\}$), so no such subset is definable from h. Such an example can be constructed on any C such that $|C|$ is even and at least 6; in fact, we can just use $Q(f)(h)$ for some one-to-one $f: B \to C$.

So we must look for an alternative proof of the numerical results we desire by looking more directly at the stabilizer $G = \mathrm{Sym}(B)_h$ for $h \in Q(B)$. If $|h(P)|$ is never 0 or 2 for any partition P of B, then, whenever A is a nonempty proper subset of B, $h(\{A, B\backslash A\})$ must be either $\{A\}$ or $\{B\backslash A\}$; in either case, if $s \in \mathrm{Sym}(B)$ is such that $s``A = B\backslash A$, then $s \notin G$. So G contains no permutation which maps a nonempty set to its complement; it is not hard to show that this is equivalent to stating that every element of G has a cycle of odd cardinality (e.g., a fixed point). (If s is a permutation with no odd cycle, then color the elements of each cycle alternately black and white to partition B into two sets that s interchanges. If s has a cycle of odd length m, b is a member of this cycle, and A is a subset of B such that $s``A = B\backslash A$, then $b \in A$ iff $b = s^m(b) \in B\backslash A$ iff $b \notin A$, a contradiction.) Now consider the following two statements:

Statement 4.11. *If G is a subgroup of* $\mathrm{Sym}(B)$ *such that every element of G has an odd cycle, then $\binom{|B|}{k}$ divides $|\mathrm{Sym}(B) : G|$ (i.e., $|G|$ divides $k!(n-k)!$) for some odd $k \leq |B|$.*

Statement 4.12. *If G is a subgroup of* $\mathrm{Sym}(B)$ *such that every element of G has an odd cycle, then $\Phi(|\mathrm{Sym}(B) : G|, |B|, 2, \omega)$.*

Clearly Statement 4.11 implies Statement 4.12. It turns out that Statement 4.12 is just what we need:

Proposition 4.13. *The statement "If $\gamma: \omega \to \omega$ is realized by some covariant functor F and $\gamma(0) = 0$, then γ satisfies* 1.2′(2)(b) *for $k' = 2$ and all k" is equivalent to Statement* 4.12.

Proof. First, suppose $G \subseteq \mathrm{Sym}(B)$ is a counterexample to Statement 4.12; clearly $|B| > 2$. Since no element of G maps a subset of B to its complement, there is a G-invariant way to choose one member from each pair $\{A, B\backslash A\}$ for $A \subseteq B$. (The orbits of subsets of B under G come in complementary pairs; just choose one orbit from each pair.) Define $h \in Q(B)$ by: if $|P| \neq 2$, then $h(P) = P$; if $|P| = 2$, then $h(P) = \{A\}$, where A is that member of P which is chosen above. Let G' be the stabilizer of h in $\mathrm{Sym}(B)$; then G is a subgroup of G', so $|\mathrm{Sym}(B) : G'|$ divides $|\mathrm{Sym}(B) : G|$, so it is not true that $\Phi(|\mathrm{Sym}(B) : G'|, |B|, 2, \omega)$.

Let F be the subfunctor of Q generated by h. Then $F(C) = \{F(f)(h)\colon f\colon B \to C\}$, and $C_{F(f)(h)} = f\text{“}\, h(\{f^{-1}\text{“}\,\{c\}\colon c \in f\text{“}\, B\})$ (since $K_F(C)(x) = x$ for $x \in F(C)$). If f is not one-to-one, then $0 < |C_{F(f)(h)}| < |B|$ and $|C_{F(f)(h)}| \neq 2$; if f is one-to-one, then $|C_{F(f)(h)}| = |B|$. Therefore, if $\gamma\colon \omega \to \omega$ is the function realized by F, then $\gamma(0) = \gamma(2) = 0$, $\gamma(m) = 0$ for $m > |B|$, and

$$\gamma(|B|) = |\{x \in F(B)\colon B_x = B\}| = |\{F(f)(h)\colon f \in \mathrm{Sym}(B)\}| = |\mathrm{Sym}(B) : G'|,$$

so $\Phi(\gamma(|B|), |B|, 2, \omega)$ fails. Therefore, γ violates $1.2'(2)$(b) for $k' = 2$ where k is either ω or any odd number greater than $|B|$.

Now suppose that Statement 4.12 holds, and let F be a covariant functor realizing a function γ such that $\gamma(0) = \gamma(2) = 0$. For the case $k' = 2$, $k = \omega$ of $1.2'(2)$(b), it suffices to show that, if $|B| > 2$, $x \in F(B)$, and M is the size of the orbit of x under $\mathrm{Sym}(B)$, then $\Phi(M, |B|, 2, \omega)$. Let $G \subseteq \mathrm{Sym}(B)$ be the stabilizer of x; then $M = |\mathrm{Sym}(B) : G|$. For any $A \subseteq B$ other than $\varnothing$ or B, $K_F(B)(x)(\{A, B\backslash A\})$ must be either $\{A\}$ or $\{B\backslash A\}$; hence, no element of G maps A onto $B\backslash A$. Now Statement 4.12 implies $\Phi(|\mathrm{Sym}(B) : G|, |B|, 2, \omega)$, as desired.

To prove that $1.2'(2)$(b) holds for $k' = 2$ and any odd number $k > 2$ such that $\gamma(k) = 0$, we will show that, if $|B| > k$ and x, M, G are as above, then $\Phi(M, |B|, 2, k)$. Apply Lemma 4.9 to $h = K_F(B)(x)$ to get a set $A \subseteq B$ definable from h (and hence fixed under G) such that $|A| < k$ and either $|A|$ is odd or $h(\{\{a\}\colon a \in A\} \cup \{B\backslash A\}) = \{\{a\}\colon a \in A\}$. Let G' be the set of elements of G not moving any element of $B\backslash A$ (which is a subgroup of G), and let G'' be the subgroup of $\mathrm{Sym}(A)$ corresponding to G'; then $|G'| = |G''|$, and $|G : G'|$ divides $(|B\backslash A|)!$. If $|A|$ is odd, then $\Phi(|\mathrm{Sym}(B) : G|, |B|, 2, k)$ since $\binom{|B|}{|A|}$ divides $|\mathrm{Sym}(B) : G|$, so we may assume that $|A|$ is even. Since $\gamma(0) = 0$, $h(\{B\}) = \{B\}$, so $A \neq \varnothing$. For any $A' \subseteq A$ other than $\varnothing$ or A, $h(\{A', A\backslash A', B\backslash A\})$ cannot contain $B\backslash A$ by 3.1(3), so it must be either $\{A'\}$ or $\{A\backslash A'\}$; it follows that no element of G' (and hence no element of G'') maps A' onto $A\backslash A'$. Therefore, by 4.12, $\Phi(|\mathrm{Sym}(A) : G''|, |A|, 2, \omega)$, and hence $\Phi(|\mathrm{Sym}(A) : G''|, |A|, 2, k)$ (since $|A| < k$). Since $|G|$ divides $|G''|(|B\backslash A|)!$, $\binom{|B|}{|A|}|\mathrm{Sym}(A) : G''|$ divides $\binom{|B|}{|A|}|A|!(|B\backslash A|)!/|G| = |\mathrm{Sym}(B) : G|$; since $\binom{|B|}{|A|}\binom{|A|}{m} = \binom{|B|}{m}\binom{|B|-m}{|A|-m}$ for all $m \leq |A|$, we get $\Phi(|\mathrm{Sym}(B) : G|, |B|, 2, k)$, as desired. Q.E.D.

It also turns out that Statement 4.11 is true; the proof is group-theoretic rather than combinatorial, so it is postponed until the next section. This result and Propositions 4.3, 4.10, and 4.13 give one direction of Theorem 4.1; the other direction follows from Lemma 2.7 and the following result.

Proposition 4.14. *If $\gamma\colon \omega \to \omega$ satisfies the conditions given for γ in* 1.2(2), *then γ is realized by some covariant functor F.*

Proof. By Lemma 2.7, we may assume $\gamma(0) = 0$. Define k_0, k_0', and k_0'' as in 1.2(2). The functor we construct will include two ‘spines,’ one of which is a copy of the example F_2 from §1 truncated at k_0' (or at k_0'' if $k_0'' < k_0' < k_0$ and $\overline{\Phi}(\gamma, k_0', k_0')$ fails) while the other is a copy of example F_3 truncated at

k_0 (or at k_0'' if $k_0'' < k_0' < k_0$ and $\overline{\Phi}(\gamma, k_0', k_0')$ holds). The rest of the functor will consist of small pieces, each attached to one of the spines. If this spine goes all the way up to N, then we can attach an extra piece at N so as to increase $\gamma(N)$ by 1 without affecting any other values $\gamma(n)$; if the spine has been truncated at $\tilde{k}$, however, then the piece we attach will increase $\gamma(N)$ by $\binom{N}{m}$ for some positive $m < \tilde{k}$, which will be odd for the second spine.

The given hypotheses allow us to choose numbers $l_{nm} \in \omega$ for $n \geq m \geq 1$ and $j_{nmi} \in \{1, 2\}$ for $n \geq m \geq 1$, $i < l_{nm}$, satisfying the following conditions:

(1) $\gamma(n) = \sum_{m=1}^{n} l_{nm}\binom{n}{m}$ for $n \geq 1$;

(2) if $k_0 < \omega$, then $l_{nm} = 0$ for all $n \geq m \geq k_0$;

(3) if $k_0' \geq k_0$, then $l_{nn} = \gamma(n)$ for all $n < k_0$, and $j_{nmi} = 1$ for all n, m, i;

(4) if $k_0' < k_0$, then $l_{nm} = 0$ for all $n \geq m \geq k_0'$ such that m is even;

(5) if $k_0' < k_0$ and $k_0'' \geq k_0'$, then $l_{nn} = \gamma(n)$ for all $n < k_0'$ and for all odd n such that $k_0' < n < k_0$, $j_{nn1} = 2$ for all odd n such that $1 < n < k_0'$, $j_{nmi} = 2$ for all $n \geq m \geq k_0'$ and $i < l_{nm}$, and $j_{nmi} = 1$ for all other n, m, i;

(6) if $k_0'' < k_0' < k_0$ and $\overline{\Phi}(\gamma, k_0', k_0')$ holds, then $l_{nn} = \gamma(n)$ for all $n < k_0'$, $l_{nm} = 0$ for all $n \geq m \geq k_0'$, and $j_{nmi} = 1$ for all n, m, i; and

(7) if $k_0'' < k_0' < k_0$ and $\overline{\Phi}(\gamma, k_0', k_0')$ fails (so $\overline{\Phi}(\gamma, k_0'', k_0)$ holds), then $l_{nn} = \gamma(n)$ for all $n < k_0''$, $l_{nm} = 0$ for all $n \geq m \geq k_0''$ such that m is even, $j_{nn1} = 2$ for all odd n such that $1 < n < k_0''$, $j_{nmi} = 2$ for all $n \geq m \geq k_0''$ and $i < l_{nm}$, and $j_{nmi} = 1$ for all other n, m, i.

(Note that the hypotheses for these conditions mean that we only have to satisfy (1) and (2) together with either (3) alone, (4) and (5), (4) and (6), or (4) and (7). The cases where l_{nn} is specified to be $\gamma(n)$ are trivial. In the cases where l_{nn} is specified to be 0, the hypotheses in 1.2(2) imply the existence of numbers l_{nm} meeting these conditions. The conditions clearly define j_{nmi} uniquely for each n, m, i.)

For any finite set B, let

$$F(B) = \{(A, A', i) \colon \varnothing \neq A' \subseteq A \subseteq B,\ 0 \leq i < l_{|A||A'|}\}.$$

The first spine will consist of the triples $(D, D, 0)$ for $|D|$ below the truncation limit for F_2, while the second spine consists of the triples $(D, D, 1)$ for $|D| > 1$ odd and below both truncation limits, together with $(D, D, 0)$ for all other odd $|D|$ below the truncation limit for F_3 (i.e., when $|D|$ is 1 or not below the truncation limit for F_2). (Note that the triples $(\{b\}, \{b\}, 0)$ are in both spines.) All other triples (A, A', i) form the extra pieces added on. (If such a piece includes a triple (A, A', i), it will also include all triples (A, A'', i), where $|A''| = |A'|$; this will contribute 1 to $\gamma(|A|)$ if $|A| = |A'|$, more otherwise.) The number $j_{|A||A'|i}$ indicates which spine (A, A', i) is attached to. We can now write down the exact formula for $F(f)$ for $f \colon B \to C$:

$$F(f)((A, A', i)) = \begin{cases} (f``A, f``A', i) & \text{if } f \text{ is one-to-one on } A, \\ (D, D, 1) & \text{if } f \text{ is not one-to-one on } A,\ |D| > 1, \\ & \text{and } j_{|D||D|0} \neq j_{|A||A'|i}, \\ (D, D, 0) & \text{otherwise,} \end{cases}$$

where

$$D = \begin{cases} f``A' & \text{if } j_{|A||A'|i} = 1, \\ \{c \in C \colon |A' \cap f^{-1}``\{c\}| \text{ is odd}\} & \text{if } j_{|A||A'|i} = 2. \end{cases}$$

The proof that F is a covariant functor is tedious but straightforward, so it is omitted. Given $(A, A', i) \in F(B)$, it is clear that (A, A', i) is controlled by A. But if $p, q \colon B \to C$ are one-to-one and $p``A \neq q``A$, then $F(p)((A, A', i)) \neq F(q)((A, A', i))$; hence, $B_{(A, A', i)} = A$. Therefore, the number of elements x of $F(B)$ such that $B_x = A$ is $0 = \gamma(0)$ if $A = \varnothing$ and

$$|\{(A, A', i) \colon \varnothing \neq A' \subseteq A, \ \ i < l_{|A||A'|}\}| = \sum_{m=1}^{|A|} \binom{|A|}{m} l_{|A|m} = \gamma(|A|)$$

otherwise, so F realizes γ. Q.E.D.

We should again note that most functors do not look like the ones constructed here; this construction just happens to suffice for the desired numerical results. Note that the functor F constructed here satisfies $F(\varnothing) = \varnothing$; of course, this could have been arranged using Lemma 2.6 if it had not already been true. This completes the proof of Theorem 4.1 and hence of Theorems 1.2 and 1.2$'$.

5. Proof of Statement 4.11

This section gives the proof of the following result:

Theorem 5.1 (Aschbacher). *If G is a group of permutations of a finite set of size n, and every element of G has an odd cycle, then the order of G divides $k!(n-k)!$ for some odd $k \leq n$.*

(Groups satisfying the hypothesis of Theorem 5.1 have been studied by Isbell [8] and others, but the question considered here did not arise.)

Aschbacher's proof of this theorem involved the classification of finite simple groups. The proof given here combines Aschbacher's method with an approach due to Peter Neumann which eliminates the need for the classification. The terminology and most of the notation used here are those of Aschbacher [2]; all group-theoretic results for which no references are given can be found there. A few reminders: A *2-element* of a group is an element whose order is a power of 2. A group action is *transitive* if it has only one orbit, *primitive* if it preserves no nontrivial partition, and *faithful* if it has trivial kernel. If G is a group acting on a set including a set Y, then G_Y is the pointwise stabilizer of Y in G ($G_Y = \{g \in G \colon (\forall y \in Y)\, gy = y\}$) and $N_G(Y)$ is the global stabilizer of Y ($N_G(Y) = \{g \in G \colon gY = Y\}$). If $N_G(Y) = G$, then G/G_Y is isomorphic to a permutation group G^Y on Y.

Assume throughout this section that X is a finite set of cardinality n, $S = \mathrm{Sym}(X)$ is the symmetric group on X, and G is a subgroup of S.

We will use the following result, to be proved later:

Theorem 5.2 (Aschbacher). *If G is a primitive permutation group on a finite set X of size n and $|G|$ does not divide $(n-1)!$, then one of the following holds:*

(1) *n is prime.*

(2) *G includes the alternating group on X.*

(3) *$n = 8$ and G is isomorphic to the semidirect product of $\mathbf{Z}_2^3$ with its automorphism group* $\mathrm{GL}_3(2)$. (*This group is unique up to equivalence of group actions.*)

(4) *$n = 9$ and G is isomorphic to the semidirect product of $\mathbf{Z}_3^2$ with either* $\mathrm{GL}_2(3)$ *or* $\mathrm{SL}_2(3)$.

(5) *$n = 9$ and G is isomorphic to the automorphism group of* $\mathrm{SL}_2(8)$.

Let $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$ denote the semidirect product of $\mathbf{Z}_2^3$ with $\mathrm{GL}_3(2)$. The group action in (3) above is equivalent to the group of affine maps (linear maps with constant term) from $\mathbf{Z}_2^3$ to itself; the subgroup $\mathbf{Z}_2^3$ is the group of translations $x \mapsto x + c$ for $c \in \mathbf{Z}_2^3$. If $c \neq 0$, then such a translation is a permutation of $\mathbf{Z}_2^3$ with all cycles of size 2.

Lemma 5.3. *The only normal subgroups of $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$ are $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$, $\mathbf{Z}_2^3$, and $\{1\}$.*

Proof. It will suffice to show that $\mathbf{Z}_2^3$ is the unique minimal normal subgroup of $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$ (since $(\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2))/\mathbf{Z}_2^3 \cong \mathrm{GL}_3(2)$ is simple). Since $\mathrm{GL}_3(2)$ is transitive on the nonidentity elements of $\mathbf{Z}_2^3$, $\mathbf{Z}_2^3$ is a minimal normal subgroup of $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$. Suppose K is a nontrivial normal subgroup of H; it will be enough to show that $K \cap \mathbf{Z}_2^3$ is nontrivial, since then it will have to be all of $\mathbf{Z}_2^3$ by minimality. Let ag be a nonidentity element of K, where $a \in \mathbf{Z}_2^3$ and $g \in \mathrm{GL}_3(2)$. If g is the identity, we are done; if not, some $b \in \mathbf{Z}_2^3$ is moved by g, and then $b^{-1}(ag)^{-1}b(ag)$ is a nonidentity element of $K \cap \mathbf{Z}_2^3$ (since $\mathbf{Z}_2^3$ is abelian). Q.E.D.

We now proceed to prove Theorem 5.1 by induction on n. We may assume that n is even (since otherwise we could take $k = n$) and greater than 2.

Note that the hypothesis that every element of G has an odd cycle is equivalent to the statement that every 2-element of G has a fixed point. (A 2-element without fixed points clearly has no odd cycles; if $g \in G$ has no odd cycles, and m is the largest odd divisor of the order of g, then g^m is a 2-element without fixed points.)

First, suppose G is not transitive; say $X = Y \cup Z$, where Y and Z are disjoint G-invariant nonempty sets. Let $m = |Z|$; then $|G^Z|$ divides $m!$. Also, G_Z is faithful on Y, so, if every element of G_Z has an odd cycle on Y, then by the induction hypothesis there is an odd k such that $|G_Z|$ divides $(n-m-k)!k!$. But then $|G| = |G_Z||G^Z|$ would divide $N = m!(n-m-k)!k!$, which in turn divides $\binom{n-k}{m}N = (n-k)!k!$, as desired.

Similarly, we are done if every element of G_Y has an odd cycle on Z. On the other hand, if $u \in G_Z$ has no odd cycle on Y and $v \in G_Y$ has no odd cycle on Z, then uv is an element of G with no odd cycle at all, a contradiction. This completes the case where G is not transitive.

Next, suppose G is primitive. The group G cannot contain the alternating group on X, since the alternating group contains elements with no odd cycles (e.g., the product of a 2-cycle and an $(n-2)$-cycle). Similarly, G cannot be the group in 5.2(3), since we have seen that this group contains elements with no odd cycles. Therefore, Theorem 5.2 implies that $|G|$ divides $(n-1)!$, so we are done (let $k = 1$).

Finally, suppose G is transitive but not primitive. Then there is a nontrivial

G-invariant partition of X; since G is transitive, the partition must consist of blocks of equal size. Fix such a partition $P = \{X_1, X_2, \dots, X_r\}$ into r blocks of size s so that s is as small as possible. Then $n = rs$ and $1 < r, s < n$. Let M be the stabilizer $N_S(P)$ of P in $S = \mathrm{Sym}(X)$, and let $M_i = S_{X \setminus X_i}$; then $G \le M$, $M_i \cong \mathrm{Sym}(s)$, $M_P = M_1 M_2 \cdots M_r$, and $M^P \cong \mathrm{Sym}(r)$.

Note that, for any positive integers a and b, we can consider the symmetric group on ab objects and the subgroup which preserves some partition into b blocks of size a; this subgroup has order $(a!)^b b!$, so $(a!)^b b!$ divides $(ab)!$.

Since every element of G has an odd cycle on X, every element of G^P has an odd cycle on P (if x is in an odd cycle of g on X, then the element of P containing x is in an odd cycle of $G_P g$ on P). By the induction hypothesis, there is an odd number $j \le r$ such that $|G^P|$ divides $(r-j)!j!$. But $|G_P|$ divides $|M_P| = (s!)^r$, so $|G| = |G_P||G^P|$ divides $(s!)^r(r-j)!j! = (s!)^{r-j}(r-j)!(s!)^j j!$, which in turn divides $(n-sj)!(sj)!$. We are now done if s (and hence sj) is odd, so assume that s is even.

By minimality of s, $N_G(X_i)^{X_i}$ is primitive on X_i. Since $G_P \trianglelefteq G$, $(G_P)^{X_i} \trianglelefteq N_G(X_i)^{X_i}$. If $|(G_P)^{X_i}|$ divides $(s-1)!$ for all i, then $|G_P|$ divides $((s-1)!)^r$, so G divides $((s-1)!)^r r!$, which divides $(n-r)!$, which divides $(n-1)!$, so we are done. So we may assume $|(G_P)^{X_i}|$, and hence $|N_G(X_i)^{X_i}|$, does not divide $(s-1)!$ for some i. Now Theorem 5.2 implies that either $\mathrm{Alt}(X_i) \le N_G(X_i)^{X_i}$ (where $\mathrm{Alt}(X_i)$ is the alternating group on X_i) or $s = 8$ and $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2) \cong N_G(X_i)^{X_i}$. Using Lemma 5.3 and the simplicity of $\mathrm{Alt}(X_i)$ if $s \ge 6$, we can now conclude that either $\mathrm{Alt}(X_i) \le (G_P)^{X_i}$, $s = 4$, or $s = 8$ and $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2) \cong (G_P)^{X_i}$. This has been shown for one value of i, but since G^P is transitive on P it must hold for all i.

Next, we show that $G_{X-X_i} = \{1\}$ for all i. Since $G_{X-X_i} \trianglelefteq N_G(X_i)$, $(G_{X-X_i})^{X_i} \trianglelefteq N_G(X_i)^{X_i}$, so $(G_{X-X_i})^{X_i}$ must be either $\{1\}$, $\mathrm{Alt}(X_i)$, $\mathrm{Sym}(X_i)$, $\mathbf{Z}_2^3 \cdot \mathrm{GL}_3(2)$ or its normal subgroup $\mathbf{Z}_2^3$ (with $s = 8$), or a nontrivial normal subgroup of $\mathrm{Sym}(X_i)$ or $\mathrm{Alt}(X_i)$ (with $s = 4$); in the latter case, we easily check that G_{X-X_i} must include the permutations with cycle structure $(a\ b)(c\ d)$. In all of these cases other than $\{1\}$, G_{X-X_i} contains an element with no odd cycle in X_i. If this is true for one i, then it is true for all i; if we choose one such element for each i and multiply them all together, we get an element of G with no odd cycles at all, contradicting the choice of G. Therefore, G_{X-X_i} must be $\{1\}$ for all i.

Claim. s is 2, 4, or 8 (and hence $p = 2$).

Proof. Suppose not; then $s \ge 6$ (since s is even) and the commutator subgroup D_i of M_i is isomorphic to $\mathrm{Alt}(s)$, which is a nonabelian simple group. Let $D = D_1 D_2 \cdots D_r$ and $A = G \cap D$. We know that $D_i^{X_i} \le (G_P)^{X_i}$; since D_i has no subgroup of index 2, it follows by induction on k that $D_i^{X_i} \le (G \cap D_1 \cdots D_k M_{k+1} \cdots M_r)^{X_i}$. For $k = r$ this states that $D_i^{X_i} \le A^{X_i}$, so the canonical projection from D to D_i maps A onto D_i. Now Lemma 1.4 of Aschbacher and Scott [3] states that there is a partition $Q = \{Q_1, \dots, Q_t\}$ of $\{D_1, \dots, D_r\}$ such that $A = A_1 \cdots A_t$, where A_i is a full diagonal subgroup of $\langle Q_i \rangle$ (i.e., for each D_j in Q_i, the canonical projection from A_i to D_j is a bijection). In particular, for each $i \le t$ there is a 2-element g_i of A_i which has no fixed points on any X_j such that $D_j \in Q_i$. (Given i, choose one such

j, let $h \in D_j$ be a 2-element with no fixed points on X_j, and let $g_i \in A_i$ be the unique element which projects to h. To see that this g_i has suitable projections to the other elements of Q_i, we must see that the set of 2-elements of $\mathrm{Alt}(s)$ with no fixed points is fixed under automorphisms of $\mathrm{Alt}(s)$. This is easy for $s > 6$, since then conjugation by members of $\mathrm{Sym}(s)$ gives all automorphisms of $\mathrm{Alt}(s)$ [12, §65]. For $s = 6$, note that the 2-elements of $\mathrm{Alt}(6)$ with no fixed points are the products of a disjoint 4-cycle and 2-cycle, and these are just the elements of $\mathrm{Alt}(6)$ of order 4.) Now $g = g_1 \cdots g_t$ is a 2-element of G with no fixed points, contradicting the choice of G. Q.E.D.

Recall that $|G^P|$ divides $(r-j)!j!$ for some odd $j \le r$. Since $G_{X-X_i} = \{1\}$, $|G_P|$ divides $(s!)^{r-1}$, so $|G|$ divides

$$(s!)^{r-1} j!(r-j)! = (s!)^{j-1} j!(s!)^{r-j}(r-j)!.$$

As noted before, $(s!)^{r-j}(r-j)!$ divides $(s(r-j))!$, so it divides $(s(r-j)+1)!$. If we write $(s!)^{j-1}j!$ as ab with a odd and b a power of 2, then a divides $((s-1)!)^{j-1}j!$ (since s is a power of 2), which divides $((s-1)!)^j j!$, which divides $((s-1)j)!$, which divides $(sj-1)!$. Also, b divides $(s!)^{j-1}(j-1)!$ (since j is odd), which divides $(s(j-1))!$, which divides $(sj-1)!$. Since a and b are relatively prime, $ab = (s!)^{j-1}j!$ divides $(sj-1)!$. Therefore, $|G|$ divides $(sj-1)!(n-(sj-1))!$, which is the desired result because $sj-1$ is odd. This completes the proof of Theorem 5.1 assuming Theorem 5.2.

Proof of Theorem 5.2. Suppose G is as hypothesized, n is composite, and G does not contain the alternating group; we must show that one of the last three cases in Theorem 5.2 holds. It is easy to verify that any primitive group on four elements contains the alternating group, so n must be greater than 4. Since $|G|$ does not divide $(n-1)!$, n does not divide $|\mathrm{Sym}(X) : G|$, so there is a prime power p^a which divides n but not $|\mathrm{Sym}(X) : G|$. Let P be a Sylow p-subgroup of G, and let Q be a Sylow p-subgroup of $\mathrm{Sym}(X)$ including P; then $|Q : P|$ is the largest power of p dividing $|\mathrm{Sym}(X) : G|$, so $|Q : P| < p^a$.

Now, Q has a subgroup R of order $p^{n/p}$ generated by n/p disjoint p-cycles [7, §5.9]. Then R is isomorphic to $\mathbf{Z}_p^{n/p}$, and this isomorphism maps $P \cap R$ to a subspace P' of $\mathbf{Z}_p^{n/p}$ of dimension $k = n/p - \log_p |R : P \cap R| > n/p - a$. So $a > n/p - k$; since $p^a | n$, $p^{n/p-k}$ must divide n/p, so $p^{n/p-k} \le n/p$. We can now apply the sphere-packing bound from the theory of error-correcting codes [11, Theorem 1.6], which states that an e-error-correcting p-ary linear code of length m and dimension k (i.e., a subspace of $GF(p)^m$ of dimension k in which every nonzero vector has at least $2e+1$ nonzero coordinates; here $GF(p)$ is the finite field with p elements) cannot exist unless $p^{m-k} \ge \sum_{r=0}^{e} \binom{m}{r}(p-1)^r$; comparing this inequality with the preceding one, we see that P' cannot even be 1-error-correcting, so it must contain an element with exactly one or two nonzero coordinates. Therefore, P (and hence G) contains an element which is a p-cycle or a product of two disjoint p-cycles.

If G is a primitive permutation group on n objects containing a p-cycle (p prime), and G does not include the alternating group, then $n \le p+2$; this is a result of Jordan (see Wielandt [16, Theorem 13.9]). But, in the present situation, n is a composite multiple of p, so $n \ge 2p$; this leads to $p = 2$ and $n = 4$, which we have already eliminated. Therefore, P contains no p-cycle, so $Q \ne P$ and hence $a > 1$.

So G contains a product of two disjoint p-cycles, and p^2 divides $|G|$ (since $p^2|n$ and G is transitive). If p is odd, then the main theorem of Praeger [14] implies that $p = 3$, $n = 9$, and G is one of the possibilities listed in (4) and (5). If $p = 2$, then Theorem III in §121 of Netto [13] states that n must be no larger than 8, and since we have already ruled out $n = 4$ we must have $n = 8$. Carmichael [5, Example 16, p. 165] lists the primitive groups of order 8; there are seven of them up to equivalence of group actions, of which two contain the alternating group and four have orders which divide 7!. The only remaining possibility is the one given in (3). Q.E.D.

6. Conclusion

In the course of settling the numerical questions posed in §1, we have developed some useful structure theory for functors on $\mathcal{FS}$, leading eventually to the functor Q and the morphisms K_F and their contravariant versions; these results should be useful in the further study of such functors. For example, any subfunctor of Q produces a corresponding subfunctor of F via K_F. In particular, one can look at the subfunctors F_n of F consisting of those $x \in F(B)$ which are controlled by a set of size at most n; these form an increasing sequence with limit F, and F_{n+1} can be described as an extension of F_n by a relatively simple functor [4].

One can look at related types of functors, such as functors from $\mathcal{FS} \times \mathcal{FS}$ to $\mathcal{FS}$ or functors from $\mathcal{FS}$ to the category of finite sets with a distinguished subset. (Or one can look at the category whose objects are finite sets but whose arrows from A to B are arbitrary subsets of $A \times B$, with composition defined in the natural way.) Each such functor gives rise to a numerical function, and one can again consider the problem of characterizing these functions. By developing structural results analogous to the ones given here, one might be led to solutions of these problems; and the numerical problems serve as a useful test case for whatever structure theory is developed.

Some related work: Trnková [15] and Koubek [9] study the structure of functors on the category of all sets, while functors between categories of finite-dimensional vector spaces are examined by Epstein and Kneber [6].

Acknowledgments

I would like to thank George Bergman for suggesting this problem (on a homework assignment—I did not get much other homework done in that course) and for many helpful suggestions for improving the paper. I would also like to thank Michael Aschbacher for providing (and explaining to a non-group-theorist) the original proof of Statement 4.11, Peter Neumann for the alternative approach used here to prove Theorem 5.2, and Ronald Solomon for help finding out about primitive groups of order 8.

References

1. M. Abramowitz and I. Stegun (editors), *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, National Bureau of Standards, Applied Mathematics Series, vol. 55, U. S. Government Printing Office, Washington, 1964.
2. M. Aschbacher, *Finite group theory*, Cambridge Univ. Press, Cambridge, 1986.
3. M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.
4. G. Bergman, *Functors from finite sets to finite sets*, unpublished notes.

5. R. Carmichael, *Introduction to the theory of groups of finite order*, Dover, New York, 1956.

6. D. Epstein and M. Kneber, *Functors between categories of vector spaces*, Category Theory, Homology Theory and their Applications. III, Lecture Notes in Math., vol. 99, Springer-Verlag, Berlin, 1969, pp. 154–170.

7. M. Hall, Jr., *The theory of groups*, Macmillan, New York, 1959.

8. J. Isbell, *Homogeneous games*. II, Proc. Amer. Math. Soc. **11** (1960), 159–161.

9. V. Koubek, *Set functors*, Comment. Math. Univ. Carolinae **12** (1971), 175–195; *Set functor* [sic] II—*contravariant case, ibid.* **14** *(1973)*, 47–57; *Set functors* III—*monomorphisms, epimorphisms, isomorphisms*, with J. Reiterman, *ibid.* **14** (1973), 441–455.

10. S. Mac Lane, *Categories for the working mathematician*, Graduate Texts in Math., vol. 5, Springer-Verlag, New York, 1971.

11. F. MacWilliams and N. Sloane, *The theory of error correcting codes*, North-Holland, Amsterdam, 1977.

12. G. Miller, H. Blichfeldt, and L. Dickson, *Theory and applications of finite groups*, Dover, New York, 1961.

13. E. Netto, *The theory of substitutions and its applications to algebra*, 2nd ed., Chelsea, New York, 1964.

14. C. Praeger, *Primitive permutation groups containing an element of order p of small degree, p a prime*, J. Algebra **34** (1975), 540–546.

15. V. Trnková, *Some properties of set functors*, Comment. Math. Univ. Carolinae **10** (1969), 323–352; *On descriptive classification of set-functors*. I, *ibid.* **12** (1971), 143–174; II, *ibid.* **12** (1971), 345–357.

16. H. Wielandt, *Finite permutation groups*, Academic Press, New York, 1964.

Department of Mathematics, Ohio State University, Columbus, Ohio 43210