Finite induction; Big products and sums

Near the end of the previous lecture we noted that the cardinal numbers of the points on the plane and the points on a line are equal. It is natural to ask whether the number of points in $3-$ dimensional coordinate space is also equal to the number of points on a line, and likewise for the number of points in $n-$ dimensional coordinate space. The proof of this will use a fundamental mathematical technique called ***proof by (finite) induction.***

Before doing anything further, we need to define a notion of Cartesian product of a finite indexed collection $X_1, \dots, X_n$ of sets. We already know how to do this if $n = 2$, and the general definition is recursive.

Definition. Given $X_1, \dots, X_n$ as above, the ***Cartesian product*** $X_1 \times \dots \times X_n$ is defined recursively for $n > 2$ by $(X_1 \times \dots \times X_{n-1}) \times X_n$.

We want this construction to have the following property:

Proposition (Coordinatewise equality property). *Every element of an $n-$ fold product $X_1 \times \dots \times X_n$ is given by an ordered list $(x_1, \dots, x_n)$ where $x_j \in X_j$ for all j from 1 to n. Two ordered lists $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ define the same element of the product if and only if $x_j = y_j$ for all j.*

PROOF WHEN $n = 3$. Since $X_1 \times X_2 \times X_3 = (X_1 \times X_2) \times X_3$ by definition, every point in the set can be uniquely written as an ordered pair (w, z) where $w \in X_1 \times X_2$ and $z \in X_3$ are uniquely determined. But every element w of $X_1 \times X_2$ can be uniquely expressed as an ordered pair (x, y) where $x \in X_1$ and $y \in X_2$. Therefore we have obtained an ordered triple of elements $x \in X_1$, $y \in X_2$, and $z \in X_3$. To see that these coordinates are uniquely determined, suppose we have $((x,y),z) = ((a,b),c)$. The properties of a $(2-$ fold) Cartesian first product imply that $(x,y) = (a,b)$ and $z = c$, and similarly $(x,y) = (a,b)$ implies that $x = a$ and $y = b$.■

Corollary. *The cardinalities of $\mathbb{R}$ and $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ are equal.*

Proof. We know that there is a $1-1$ onto map h from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. We claim that the function $k(x,y,z) = h(h(x,y),z)$ is also a $1-1$ onto mapping. To see that

k is $1 - 1$, suppose that $k(x, y, z) = k(x', y', z')$. Since h is $1 - 1$, we first know that $h(x, y) = h(x', y')$ and $z = z'$, and from these we know that $x = x'$ and $y = y'$. To see that k is onto, we first know that every $a \in \mathbb{R}$ is $h(w, z)$ for some w and z in $\mathbb{R}$, and similarly $w = h(x, y)$ for some $x, y \in \mathbb{R}$. Combining these, we have $a = h(w, z) = h(h(x, y), z) = \mathrm{k}(x, y, z)$ for some x, y and z.■

One can proceed similarly, using the $3 -$ fold case to derive the $4 -$ fold case, then using the $4 -$ fold case to derive the $5 -$ fold case, and so on. Such patterns arise repeatedly in the mathematical sciences, and they me be treated in a unified manner as follows:

WEAK PRINCIPLE OF FINITE INDUCTION. *Suppose that we are given a sequence of statements S_n where n runs through all positive integers, and assume also that the following hold:*

1. *Statement S_1 is true.*
2. *For all $n \in \mathbb{N}_+$, if Statement S_n is true then Statement S_{n+1} is also true.*

Then all of the statements S_n are true.

JUSTIFICATION. If not all of the statements are true, then there is a least positive integer m such that S_m is false; such an integer must exist because the set of positive integers is well $-$ ordered. By the first condition on the sequence $\{S_n\}$, we know that $m > 1$. Since m is minimal and $m > 1$, we know that $m - 1 \geq 1$ and therefore S_{m-1} must be true. By the second condition on the sequence $\{S_n\}$, the truth of S_{m-1} implies that S_m is also true. However, we assumed that S_m was false, so this yields a contradiction. The source of the contradiction was the assumption that some Statement S_n was false, so we are forced to conclude that all the statements S_n are true.■

In many cases the the indexing variable n for S_n may range over all integers greater than or equal to some fixed nonnegative integer M (for example, $M = 0$). The principle also holds in these instances because the set of integers $\geq M$ is also well $-$ ordered; the only change is the need to assume that the initial statement S_M is true.

NOTE. The similarity between the phrases "mathematical induction" and "inductive reasoning" may suggest that the first concept is a form of the second, but ***this is <u>not</u> the case.*** Inductive reasoning is certainly different from deductive reasoning, but ***mathematical induction is actually a form of <u>deductive</u> reasoning.***

Formally, the difference between mathematical induction and inductive reasoning sis that the latter would check the first few statements, say S_1, S_2, S_3, S_4, and then conclude that S_n holds for all n. The crucial inductive step, "S_n implies S_{n+1}," is missing. Needless to say, inductive reasoning does not constitute a proof in the strict sense of deductive logic.

__Visual Model.__ In effect, ***<u>mathematical induction allows one to prove an infinite list of statements</u>***, say S_1, S_2, S_3, ... , ***<u>with an argument that has only finitely many steps</u>***. It may be helpful to visualize this in terms of the domino effect; if you have a long row of dominoes standing on end, you can be sure of two things:

1. The first domino can be pushed over.
2. Whenever a domino falls, then its next neighbor will also fall.

Under these conditions, we know that ***each one of the dominos in the long row will eventually fall*** if the first one is nudged down in the right direction.

__Classical Example.__ Let S_n be the familiar formula for the sum of the first n odd positive integers:

$$1 + 3 + 5 + ... + (2n-1) = n^2$$

In this case the first statement S_1 is $1 = 1^2$, the statement S_2 is $1+3 = 2^2$, the statement S_3 is $1+3+3 = 3^2$, and so on. The proof by mathematical induction has two basic steps:

Proving that the first statement S_1 is true.

Proving that for each value of n such that $n \geq 1$, if S_n is true, then so is the next statement S_{n+1}.

__Proof of the example by induction.__ The statement S_1 is simply $1 = 1^2$, and hence it is obviously true. Let's assume we know that S_n is also true for an arbitrary $n \geq 1$, so that we have the equation $1 + 3 + 5 + ... + (2n-1) = n^2$. The next step in mathematical induction is to derive S_{n+1} from S_n. To do this, we note that

$$\begin{aligned} 1+3+...+(2n-1)+(2n+1) &= [1+3+...+(2n-1)] + (2\mathrm{n}+1) \\ &= n^2 + (2n+1) \\ &= (n+1)^2 \end{aligned}$$

which shows that S_{n+1} is also true because $2n+1 = 2(n+1)-1$. Therefore S_n is true for all n and we have proven the general formula by mathematical induction.■

Frequently the verification of the first statement in a proof by induction is fairly easy or even trivial, but ***it is absolutely essential to include an explicit statement about the truth of the initial case*, AND ALSO *it is important to be sure that the inductive step works for every statement in the sequence*.** If these are not done, the final conclusion may be false and in some cases downright absurd.

Application to finite products

We shall now use the Weak Principle of Finite Induction to prove the statements about finite products at the beginning of this lecture.

<u>Proposition (Coordinatewise equality property).</u> *Every element of an $n -$ fold product $X_1 \times \dots \times X_n$ is given by an ordered list $(x_1, \dots, x_n)$ where $x_j \in X_j$ for all j from 1 to n. Two ordered lists $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ define the same element of the product if and only if $x_j = y_j$ for all j.*

<u>PROOF.</u> We already have proofs when $n = 2$ or 3, so let us assume the result is true for $(n-1) -$ fold products where $n > 3$ (in fact, the proof also works for $n = 2$ or 3, but this need not concern us).

Since $X_1 \times \dots \times X_n = (X_1 \times \dots \times X_{n-1}) \times X_n$ by definition, every point in this set can be uniquely written as an ordered pair (w, z) where $w \in X_1 \times \dots \times X_{n-1}$ and $z \in X_n$ are uniquely determined. But every element w of $X_1 \times \dots \times X_{n-1}$ can be uniquely expressed as an ordered list $(x_1, \dots, x_{n-1})$ where $x_j \in X_j$ for all j from 1 *to* $n - 1$. Therefore we have obtained an ordered list of elements $x_j \in X_j$ (where $j < n$) and $z \in X_n$. To see that these coordinates are uniquely determined, suppose we have $((x_1, \dots, x_{n-1}), z) = ((y_1, \dots, y_{n-1}), u)$. Then we have $z = u$ and $(x_1, \dots, x_{n-1}) = (y_1, \dots, y_{n-1})$ by the properties of a ($2 -$ fold) Cartesian product and $x_j = x_j$ (for $j < n$) by the inductive hypothesis. These equations combine to show that the corresponding coordinates are equal in the ($n -$ fold) Cartesian product.■

<u>Corollary.</u> *For all positive integers n, the cardinalities of $\mathbb{R}$ and $\mathbb{R}^n = \mathbb{R} \times \dots \text{x}\, \mathbb{R}$ (with n factors) are equal.*

<u>PROOF.</u> This is another proof by induction. Let S_n be the statement that the cardinalities of $\mathbb{R}$ *and* $\mathbb{R}^n$ are equal. We know that S_n is true if $n = 1, 2$ or 3.

Assume S_n is true. Then we have a $1-1$ onto mapping $f{:}\colon \mathbb{R}^n \rightarrow \mathbb{R}$, and this yields a $1-1$ correspondence $g\colon \mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ defined by $g(\mathbf{s}, t) = (f(w), t)$. If we compose this with a $1-1$ correspondence $g\colon \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, the resulting composite $h \circ g$ will be a $1-1$ correspondence from $\mathbb{R}^{n+1}$ to $\mathbb{R}$ and hence all of the statements S_n are true by finite induction.■

Example. (Somewhat more difficult than the others). Consider the following defective "proof" that a nonempty finite set contains as many elements as one of its proper subsets. This statement is vacuously true for the empty set, so assume it is true for a set with k elements. Let S be a set with $k+1$ elements; we need to show that some proper subset of S contains the same number of elements as S. Let T be obtained from S by removing one element x, and let U be a proper subset of T such that $|T| = |U|$, and let V be the proper subset of S obtained by adding x to U. Since we also know that $|S| = |T| + 1$ and $|V| = |U| + 1$ we conclude that $|S| = |V|$.??

This is obviously an absurd conclusion, so the point here is to ask, "*How did this happen*?" In fact, ***the inductive step we have given is valid for all values of k*** ***EXCEPT*** ***for the case $k = 0$.*** When $k = 0$ the argument breaks down because T will be the empty set, so it is not possible to construct the subset U by removing an element from T.

There are some instances where one uses a variant of the principle of mathematical induction stated above; namely, one replaces the assumption in the second step with a stronger hypothesis that S_m is true for **ALL** $m < n+1$ and not just for $m = n$.

STRONG PRINCIPLE OF FINITE INDUCTION. *Suppose that we are given a sequence of statements S_n where n runs through all positive integers, and assume also that the following hold:*

1. *Statement S_1 is true.*
2. *For all $n \in \mathbb{N}_+$, if Statement S_m is true for* **ALL** *$m \leq n$ then Statement S_{n+1} is also true.*

Then all of the statements S_n are true.

JUSTIFICATION. If not all of the statements are true, then there is a least positive integer m such that S_m is false; such an integer must exist because the set of positive integers is well – ordered. By the first condition on the sequence $\{S_n\}$, we have $m-1 \geq 1$ and therefore S_k must be true for all $k < m$. By the second condition on the sequence $\{S_n\}$, the truth of S_k for all $k < m$ implies that S_m is also true. However, we assumed that S_m was false, so this yields a contradiction. The source of the contradiction was the assumption that some Statement S_n was false, so we are forced to conclude that all the statements S_n are true.■

Example. Let $\mathbf{A}$ be one of the standard number systems, and let $\mathbf{A}[t]$ be the polynomial algebra of all polynomials $p(t) = a_n t^n + \ldots + a_1 t + a_0$ with coefficients in $\mathbf{A}$. We shall say that the polynomial $p(t)$ has ***positive degree*** if the polynomial is not constant, and in this case the ***degree*** of the polynomial is the largest value of n such that $a_n \neq 0$. We shall also say that a polynomial of positive degree is ***irreducible*** if it cannot be written as a product of two other polynomials, both of positive degree. Consider the following problem:

Prove that every polynomial of positive degree is a product of irreducible polynomials.

In order to avoid semantic difficulties, we shall assume that an irreducible polynomial is a product with only one factor (namely, itself).

Proof using the strong principle of finite induction. Let S_n be the statement that every polynomial of positive degree n is a product of irreducible polynomials. The first thing to do is prove that S_1 is true. This requires a digression: The product of a polynomial of degree d and a polynomial of degree e is a polynomial of degree $d+e$; if $f(t) = a_d t^d +$ (TERMS OF LOWER DEGREE) and $g(t) = b_e t^e +$ (TERMS OF LOWER DEGREE) with a_d and b_e nonzero, then $f(t)g(t) = a_d b_e t^{d+e} +$ (TERMS OF LOWER DEGREE) and the product $a_d b_e$ is also nonzero. All this is relevant to proving S_1, for it implies that the product of two polynomials of positive degree must be a polynomial of degree at least 2. Therefore a polynomial of degree 1 must always be irreducible and hence S_1 is true.

Assume now that the statements S_m are true for all m between 1 and $n-1$ for some $n > 1$, and let $p(t)$ be a polynomial of degree n. If a polynomial of degree n is irreducible, then by our language convention the conclusion of S_n is true for that polynomial. On the other hand, if $p(t) = q(t)r(t)$ where q and r have positive degrees, then the degrees of q and r must be strictly less than n. Therefore both q and r are products of irreducible polynomials, say $q = q_1 \ldots q_a$ and $r = r_1 \ldots r_b$. We then have $p = q \cdot r = q_1 \ldots q_a r_1 \ldots r_b$ is a factorization of p into irreducible polynomials, and this completes the proof of all the statements S_n by finite induction.■

NOTE. The preceding argument does not prove any sort of uniqueness for the factorization into irreducible polynomials. However, for most number systems one does have uniqueness by results of C. F. Gauss.

Big product and sum constructions

We would like to give a construction for Cartesian product which is similar to the construction of big unions and intersections. One goal is to have a general construction of finite products which does not depend upon insertion of parentheses, avoiding questions whether anything would change significantly if we defined a threefold product as $A \times (B \times C)$ instead of $(A \times B) \times C$. In some more advanced contexts such questions require serious attention, but for our purposes they can be ignored.

Definition. Let $\{X_a \mid a \in A\}$ be an indexed family of nonempty sets. Then the **(*big*) *Cartesian product***

$$\prod_{a \in A} X_a$$

is a subset of $A \times \left(\cup_{a\in A} X_a\right)$ given by all graphs of functions $y : A \rightarrow \cup_{a\in A} X_a$ such that $y(a) \in X_a$ for all $a \in A$. Frequently we shall say that $y(a)$ is the $a -$ ***coordinate*** of y.

The form of the definition was chosen so that if W_a is a nonempty subset of X_a for each $a \in A$ then $\Pi_{a \in A} W_a$ will be a subset of $\Pi_{a \in A} X_a$.

Special cases. If $A = \{1, 2\}$ then the big Cartesian product is all functions y from $\{1, 2\}$ to $X_1 \cup X_2$ such that $y_1 \in X_1$ and $y_2 \in X_2$. Thus for nearly all practical purposes the big Cartesian product behaves like the previously defined (ordinary twofold) Cartesian product; however, one this is not the mathematical definition of a twofold Cartesian product because the concept of a function was described in terms of the twofold product. When $A = \{1, 2, 3\}$ the big Cartesian product is all functions $y:\{1, 2, 3\} \rightarrow X_1 \cup X_2 \cup X_3$ such that $y_1 \in X_1$, $y_2 \in X_2$ and $y_3 \in X_3$.

The big Cartesian product has the following property analogous to the twofold and finite Cartesian products:

Proposition. *In the setting above, suppose that y and z belong to ΠX_a. Then $y = z$ if and only if $y_\beta = z_\beta$ for all $\beta \in A$.*

This follows because y *and* z are defined as functions with domain A.■

In a previoius lecture we defined a ***<u>disjoint union</u>*** (or ***<u>disjoint sum</u>***) $A \sqcup B$ of two sets A and B. There is also a corresponding notion of big disjoint sum for an indexed family $\{X_a \mid a \in A\}$.

<u>**Definition.**</u> Let $\{X_a \mid a \in A\}$ be an indexed family of nonempty sets. Then the **(*bi*g) *disjoint sum***

$$\coprod_{a \in A} X_a$$

is a subset of $\left(\cup_{a \in A} X_a\right) \times A$ given by the union of the subsets $X_a \times \{a\}$ where a runs through all the elements of A. The large symbol at the left is an upside down capital Greek Pi; the reason for this notation is that the Cartesian product and disjoint union are complementary (or dual) to each other in some abstract sense.

By construction the disjoint sum contains a copy of X_a for each a, and if $a \neq b$ then the copies of X_a and X_b are disjoint (since the second coordinates differ).

Note that if $A = \{1, 2\}$ then this definition reduces to the previous definition of the twofold disjoint union $X_1 \sqcup X_2$.