Ex. 2.7. Why are sums like $\sum_{i=2}^{7} i^2$ or $\sum_{i\in\{2,4,6\}} i^2$

or $\sum_{\substack{i\in\{1,2,\ldots,n\};\\ i \text{ is odd}}} i^2$ well-defined?

~~Exa~~ Generally: why is $\sum_{s\in S} a_s$, where S is a finite set

and $(a_s)_{s\in S}$ is a family of numbers, well-defined?

Explanation: • A number is an element of $\mathbb{A}$, where

$\mathbb{A}$ is either $\mathbb{N}$ or $\mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$.

• A family ~~ff~~ $(a_s)_{s\in S}$ of numbers (indexed by a set S)

is a choice of a number a_s for each $s\in S$.

(For example: a family indexed by $\{2,4,6\}$ is a choice

of a number a_2, a number a_4, & a number a_6.)

For example,

is $\displaystyle\sum_{s\in\{-2,-1,0,1,2\}} s^3$ equal to $\left(\left(\left((-2)^3 + (-1)^3\right) + 0^3\right) + 1^3\right) + 2^3$

or equal to $\left(\left(\left((-2)^3 + 2^3\right) + (-1)^3\right) + 1^3\right) + 0^3$?

Why are these two sums equal?

Idea: To define $\displaystyle\sum_{s\in S} a_s$ (for a finite set S & a family $(a_s)_{s\in S}$ of numbers), use recursion:

- if $S=\emptyset$, set $\displaystyle\sum_{s\in S} a_s = 0$;
- if $S\neq\emptyset$, then pick $t\in S$, and set $\displaystyle\sum_{s\in S} a_s = a_t + \sum_{s\in S\setminus\{t\}} a_s$.

But why is this well-defined, i.e. why doesn't choice of t matter?

<u>Thm. 2.8 (General commutativity).</u> The above definition is well-defined; i.e., all choices of t lead to the same result.

To make this more rigorous define a set of numbers $\operatorname{Sums}_{s\in S}(a_s)$ for any finite set S & any family $(a_s)_{s\in S}$ of numbers

as follows:

- if $S=\emptyset$, set $\operatorname{Sums}_{s\in S}(a_s)=\{0\}$.
- if $S\neq\emptyset$, then $\operatorname{Sums}_{s\in S}(a_s)=\{a_t+w \mid t\in S,\ w\in \operatorname{Sums}_{s\in S\setminus\{t\}}(a_s)\}$.

Then, Thm. 2.8 becomes:

Thm. 2.8': For any finite set S & any family $(a_s)_{s\in S}$ of numbers, $\operatorname{Sums}_{s\in S}(a_s)$ is a 1-element set.

Proof of Thm. 2.8': "Induction on $|S|$":

For each $n \in \mathbb{N}$, we'll let $\mathcal{A}(n)$ be the following statement:

$$\left(\text{For any } n\text{-element set } S \text{ \& any family } (a_s)_{s\in S}, \ \operatorname{Sums}_{s\in S}(a_s) \text{ is a } 1\text{-element set} \right).$$

Then, $\mathcal{A}(0)$ clearly holds (because if $n=0$, then $S=\emptyset$, so $\operatorname{Sums}_{s\in S}(a_s)=\{0\}$).

Now, need to prove: if $\mathcal{A}(n)$, then $\mathcal{A}(n+1)$.

So fix $n \in \mathbb{N}$. Assume $\mathcal{A}(n)$ is true. (I.e., any family of n numbers has only one sum.)

Now, let S be an $(n+1)$-element set. Let $(a_s)_{s\in S}$ be a family of numbers, we must prove that $\operatorname{Sums}_{s\in S}(a_s)$ is a 1-element set.

Clearly, $|S| = n+1 > 0$, so $S \neq \emptyset$, so $\exists\, p \in S$. Fix p. Moreover, by $\mathcal{A}(n)$, the set $\operatorname{Sums}_{s\in S\setminus\{p\}}(a_s)$ is a 1-element set. Let w_p be its one element.

Then, $a_p + w_p \in \operatorname{Sums}_{s \in S} (a_s)$.

So $\operatorname{Sums}_{s \in S} (a_s)$ has ≥ 1 element.

Now, let us prove that it has ≤ 1 element.

Let $a_q + w_q$ and $a_r + w_r$ be two of its elements (with $q \in S$, $w_q \in \operatorname{Sums}_{s \in S \setminus \{q\}} (a_s)$, $r \in S$, $w_r \in \operatorname{Sums}_{s \in S \setminus \{r\}} (a_s)$).

We want to prove: $a_q + w_q = a_r + w_r$.

If $q = r$, then $w_q = w_r$ because $\mathcal{A}(n)$ shows that $\operatorname{Sums}_{s \in S \setminus \{q\}} (a_s)$ is a 1-element set in this case. So $a_q + w_q = a_r + w_r$.

If $q \neq r$, then pick any $w_{q,r} \in \operatorname{Sums}_{s \in S \setminus \{q,r\}} (a_s)$. (This exists, since the set is nonempty, as can be easily seen by induction.)

Then, $a_r + w_{q,r} \in \operatorname{Sums}_{s \in S \setminus \{q\}} (a_s)$, and thus $w_q = a_r + w_{q,r}$, since $\operatorname{Sums}_{s \in S \setminus \{q\}} (a_s)$ is a 1-element set.

Similarly, $w_r = a_q + w_{q,r}$.

Thus, $a_q + w_q = a_q + (a_r + w_{q,r})$

$$\underset{\text{associativity}}{=} (a_q + a_r) + w_{q,r}$$

$$\underset{\text{commutativity}}{=} (a_r + a_q) + w_{q,r}$$

$$\underset{\text{associativity}}{=} a_r + (a_q + w_{q,r}) = a_r + w_r.$$

In either case, we get $a_q + w_q = a_r + w_r$.

Thus, $\operatorname{Sums}_{s \in S}(a_s)$ has ≤ 1 element.

$\Longrightarrow$ $\operatorname{Sums}_{s \in S}(a_s)$ has exactly 1 element.

Thus, $\mathcal{A}(n+1)$ holds. So, by Ind. Princ. 2.1, we conclude that $\mathcal{A}(n)$ holds $\forall n$. In other words, Thm. 2.8' is proven. $\square$

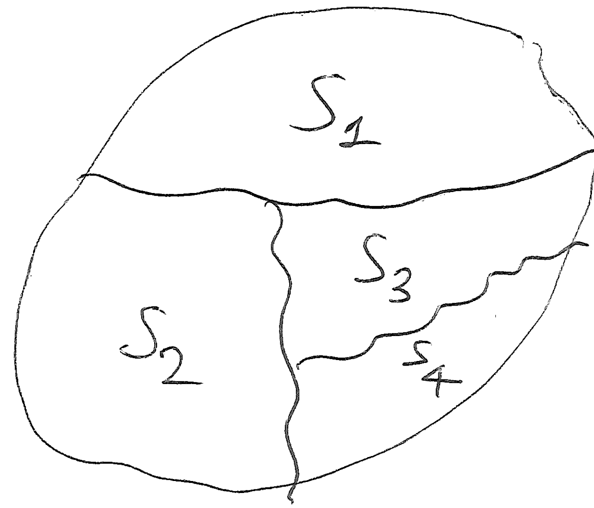
See, e.g., [detnotes, Ch. 1] for lots of formulas for summation signs. One example:

Thm. 2.9 (Splitting a sum). Let S be a finite set. Let ~~Assume that~~ $(S_1, \ldots, S_k)$ be a decomposition of S (i.e., ~~the~~ $S_1, S_2, \ldots, S_k$ are subsets of S such that each element of S lies in exactly one of them).

Let $(a_s)_{s \in S}$ be a family of numbers.

Then,

$$\sum_{s \in S} a_s = \sum_{s \in S_1} a_s + \sum_{s \in S_2} a_s + \cdots + \sum_{s \in S_k} a_s .$$



Proof idea. Induction on $|S|$. In the induction step, pick any $t \in S$, and pluck out a_t from both sides. $\square$

2.2. Shifted induction

Induction principle 2.10. Fix $g \in \mathbb{Z}$. Set $\mathbb{Z}_{\geq g} = \{g, g+1, g+2, \dots\}$.
For each $n \in \mathbb{Z}_{\geq g}$, let $\mathcal{B}(n)$ be a logical statement.

Assume:
- $\mathcal{B}(g)$ holds.
- $\forall n \in \mathbb{Z}_{\geq g}$, if $\mathcal{B}(n)$ holds, then $\mathcal{B}(n+1)$ holds.

Then, $\mathcal{B}(n)$ holds $\forall n \in \mathbb{Z}_{\geq g}$.

Proof. ~~A~~ Apply Principle 2.1 to $\mathcal{A}(n) := \mathcal{B}(n+g)$. $\square$

Example 2.11. Recall ~~the~~ ToH.

Prop. 2.12. $\forall n \geq 1$ $\forall k \geq 2^n - 1$, we can solve the n-disk ToH in k steps.

Proof. Let $\mathcal{B}(n) = (\forall k \geq 2^n - 1$, ~~we~~ we can solve the n-disk ToH in k steps).

We must prove this $\forall n \geq 1$.

$\mathcal{B}(1)$ is true (just move the disk around between ~~steps~~ pegs 1, 2, then send it to peg 3 at the last step).

Now, let $n \in \mathbb{Z}_{\geq 1}$, and assume $\mathcal{B}(n)$ holds.

Why does $\mathcal{B}(n+1)$ hold?

Let $k \geq 2^{n+1} - 1$. We must show how to ~~the~~ solve the $(n+1)$-disk ToH in k steps.

Meanwhile, $\mathcal{B}(n)$ holds, so that

(1) $\forall \ell \geq 2^n - 1$, we can solve the n-disk ToH in ℓ steps.

Now,

- first, move the disks $1, 2, .., n$ to peg 2 in $2^n - 1$ steps. (This can be done by (1), applied to $\ell = 2^n - 1$.)
- then, move disk $n+1$ to peg 3 (in 1 step),
- ~~then~~ then, move disks $1, 2, .., n$ to peg 3 in $k - 2^n$ steps. (This can be done by (1), applied to $\ell = k - 2^n$, because $k - 2^n \geq 2^n - 1$ (since $k \geq 2^{n+1} - 1$).

So $(n+1)$-disk ToH is solved in k steps. Thus, $\mathcal{B}(n+1)$ holds. $\square$

2.3. Limited / bounded induction

Induction principle 2.13. Fix $p, q \in \mathbb{Z}$ with $p \leq q$.

For each $n \in \{p, p+1, \dots, q\}$, let $\mathcal{C}(n)$ be a log. statement.

Assume:
- $\mathcal{C}(p)$ holds,
- $\forall n \in \{p, p+1, \dots, q-1\}$, if $\mathcal{C}(n)$ holds, then $\mathcal{C}(n+1)$ holds.

Then $\mathcal{C}(n)$ holds $\forall n \in \{p, p+1, \dots, q\}$.

Proof. Apply Principle 2.10 to $g = p$ and $\mathcal{B}(n) = ($if $n \leq q$, then $\mathcal{C}(n))$. $\square$

Example 2.13. 30 socks are hanging from a clothesline: 15 white socks (W) & 15 black socks (B).

Show that you can find 10 consecutive socks, among which 5 are W and 5 are B.

(Ex:

— W W B W W B B B B B $\boxed{\text{B W W B W B W B B W}}$ W B B W W W B W B W —)

Idea: Proof by contradiction. (So assume $\nexists$ such 10 socks.)

For each $i \in [21]$, let

$$b_i = (\#\text{ of black socks among the socks } i, i+1, \dots, i+9) - 5.$$

By assumption, $b_i \neq 0 \ \forall i$.

However, $b_1 + b_{11} + b_{21} =$ (# of all black socks) $- 15 = 0$.

Now, WLOG assume $b_1 > 0$ (otherwise, flip all colors).

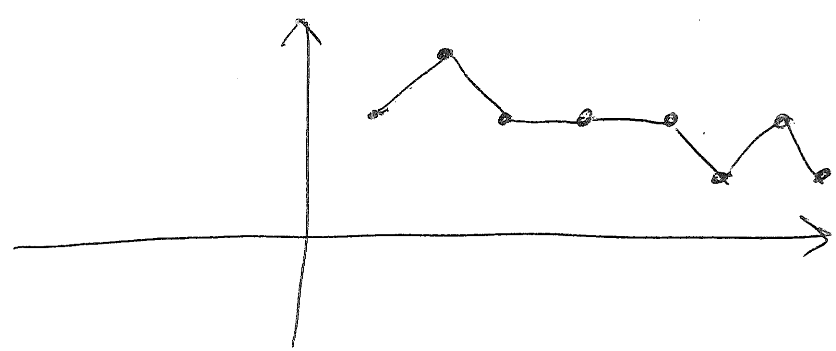
Furthermore, for every $i \in [20]$,

$$b_{i+1} - b_i = \begin{cases} 1 & \text{if sock } i+10 \text{ is black but sock } i \text{ is white,} \\ -1 & \text{if sock } i+10 \text{ is white but sock } i \text{ is black,} \\ 0 & \text{otherwise} \end{cases}$$

$\Rightarrow |b_{i+1} - b_i| \leq 1$.

So we have a sequence $(b_1, b_2, \dots, b_{21})$ of integers such that

- $b_i \neq 0 \ \forall i$,
- $b_1 > 0$,
- $|b_{i+1} - b_i| \leq 1$.



Claim: $b_i > 0 \ \forall i$.

This follows from:

Lem. 2.14 (Discrete IVT / "Discrete continuity")

Let $(b_1, b_2, \ldots, b_q)$ be a sequence of integers such that

- $b_i \neq 0 \quad \forall i$,
- $b_1 > 0$,
- $|b_{i+1} - b_i| \leq 1 \quad \forall i \in [q-1]$.

Then $b_i > 0 \quad \forall i$.

Proof. For each $n \in [q]$, let $\mathcal{C}(n)$ be the statement $(b_n > 0)$.
Use Induction Principle 2.13 to prove $\mathcal{C}(n)$ holds $\forall n$.
$\mathcal{C}(1)$ holds (since $b_1 > 0$).
Now let $n \in [q-1]$. Assume $\mathcal{C}(n)$ holds.
We must prove $\mathcal{C}(n+1)$ holds.
We have $b_n > 0$ (since $\mathcal{C}(n)$ holds) $\Rightarrow$ $b_n \geq 1$ (since $b_n \in \mathbb{Z}$).
Now assumption yields $|b_{n+1} - b_n| \leq 1$, so $b_{n+1} \geq \underbrace{b_n}_{\geq 1} - 1 \geq 1 - 1 = 0$.
But assumption yields $b_{n+1} \neq 0$. Hence $b_{n+1} > 0$. Thus, $\mathcal{C}(n+1)$ holds.
So Principle 2.13 yields $\mathcal{C}(n) \ \forall n$. Hence Lem. 2.14 is proven. $\square$

Back to our example, $b_i > 0 \ \forall i$.

So $b_1 + b_{11} + b_{21} > 0+0+0 = 0$, contradicting $b_1 + b_{11} + b_{21} = 0$.

So we have proven $\exists$ 10 consecutive socks with 5 W & 5 B.

Variants: what if

40 socks (20 W & 20 B), and we want 10 consec. (5 W & 5 B)? YES.

38 socks (19 W & 19 B), —— 10 —— ? YES.

[Proof: $b_1 + b_{11} + b_{21} + b_{29} \in \{-1, 0, 1\}$.
But $b_i > 0$ so $b_i \geq 1$ so $b_1 + b_{11} + b_{21} + b_{29} \geq 1+1+1+1 = 4$. $\lightning$]

8 socks (4 W & 4 B), —— 6 consec. (3 W & 3 B)? NO.

[Ex: B B W W W W B B.]

See HW2 for general results.

2.4. Strong induction

Induction principle 2.16. ~~Let $A(n)$~~ Let $g \in \mathbb{Z}$.

Let $A(n)$ be a statement for all $n \in \mathbb{Z}_{\geq g}$.

Assume that: • $\forall n \in \mathbb{Z}_{\geq g}$, if ($A(m)$ holds $\forall m < n$),
then $A(n)$ holds.

Then, $A(n)$ holds $\forall n \in \mathbb{Z}_{\geq g}$.

Remark: There is no "explicit" induction base.
In other words, we don't need to assume $A(g)$.
Instead, $A(g)$ ~~holds~~ follows from our assumption
"if ($A(m)$ holds $\forall m<n$), then $A(n)$ holds",
because this assumption, applied to $n=g$, says
"if $\underbrace{(A(m) \text{ holds } \forall m<g)}_{\text{This assumes nothing}}$, then $A(g)$ holds",

which is the same as saying "$A(g)$ holds".

Thus, a strong induction needs no induction base.
Often, however, ~~the~~ the proof of the induction step has to distinguish between cases $n=g$ & $n>g$, and then the first case is called an induction base.

For example, see [LeLeMe, §5.2].