Strong Induction

CMSC 250

Strong Induction: The principle

- Let us recall the weak induction principle for a moment

Strong Induction: The principle

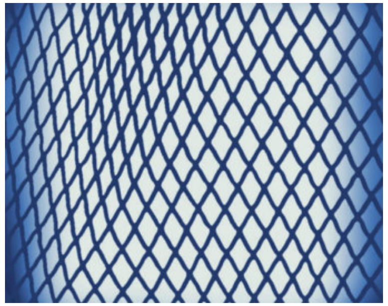
- Let us recall the weak induction principle for a moment
- The strong induction principle is different in only one thing: Instead of depending on just $P(k)$ to deduce $P(k+1)$, we will depend on **many** $P(i), 0 \leq i \leq k$

Strong Induction: The principle

- Let us recall the weak induction principle for a moment
- The strong induction principle is different in only one thing: Instead of depending on just $P(k)$ to deduce $P(k+1)$, we will depend on **many** $P(i), 0 \leq i \leq k$
- Visualization:

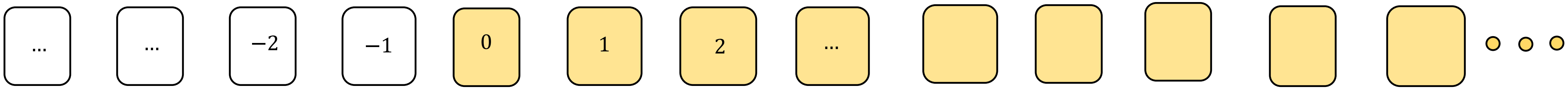
Weak Induction

Strong Induction



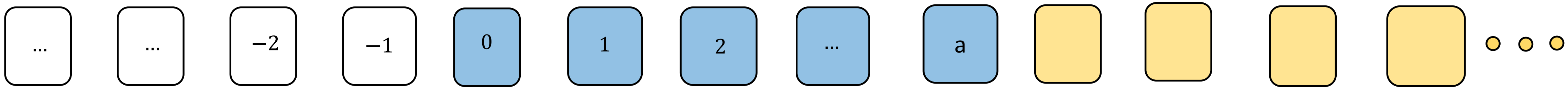
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***



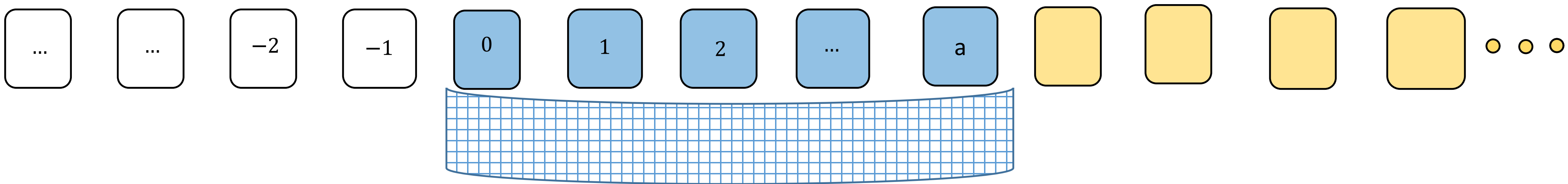
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true



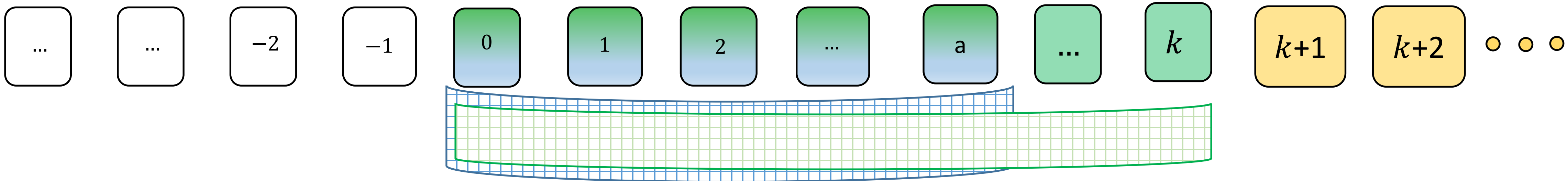
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
    a) $P(0), P(1), \ldots, P(a)$ are true



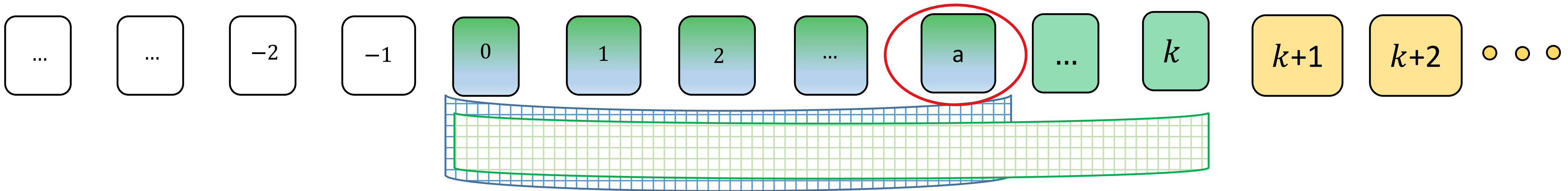
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \ldots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$



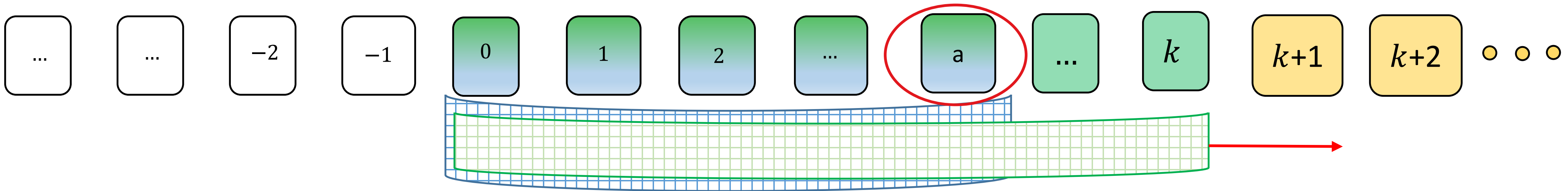
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
  $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$



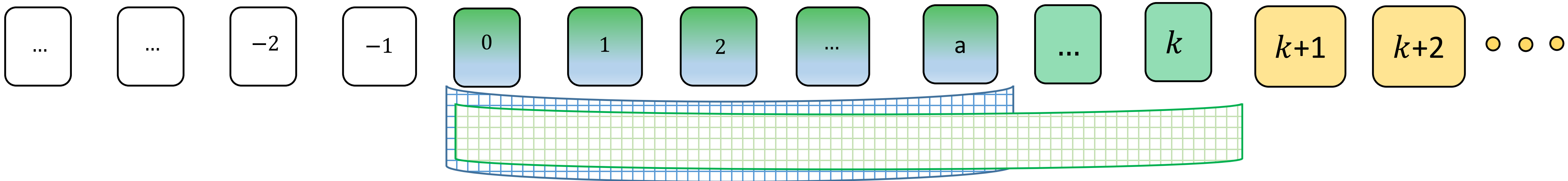
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \ldots, P(a)$ are true
  b) For $n = k \geq a$,
  $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$



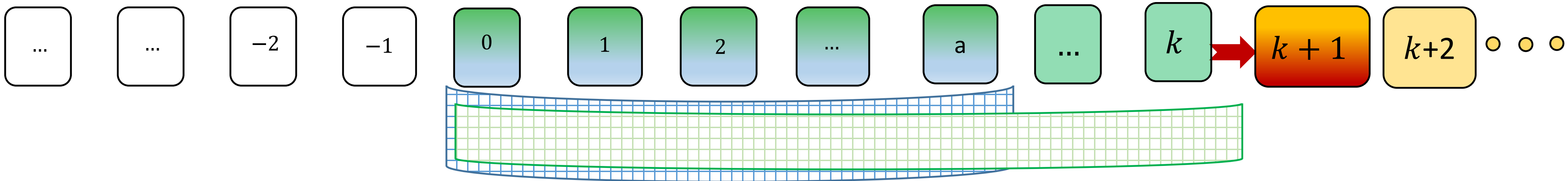
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \land P(1) \land \cdots \land P(a) \land P(a+1) \land \cdots \land P(k) \Rightarrow P(k+1)}$
- ***Then***, $P(k+1)$ is also true



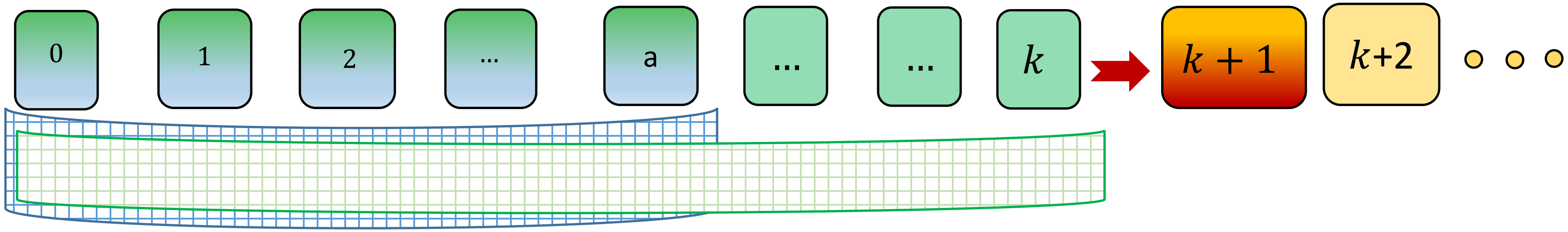
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$
- ***Then***, $P(k+1)$ is also true



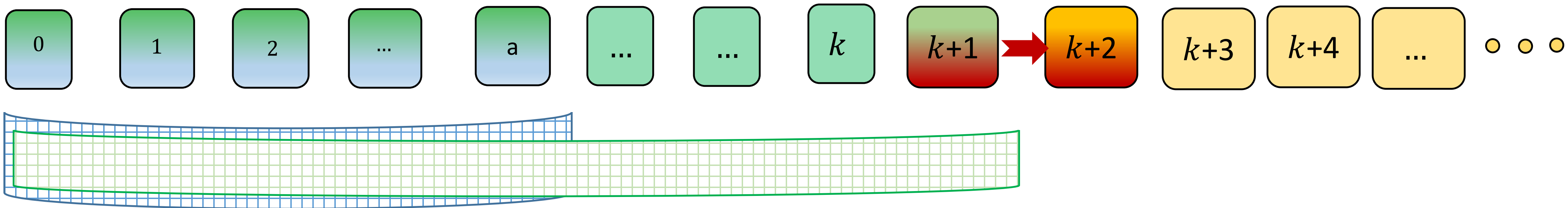
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
  $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$
- ***Then***, $P(k+1)$ is also true



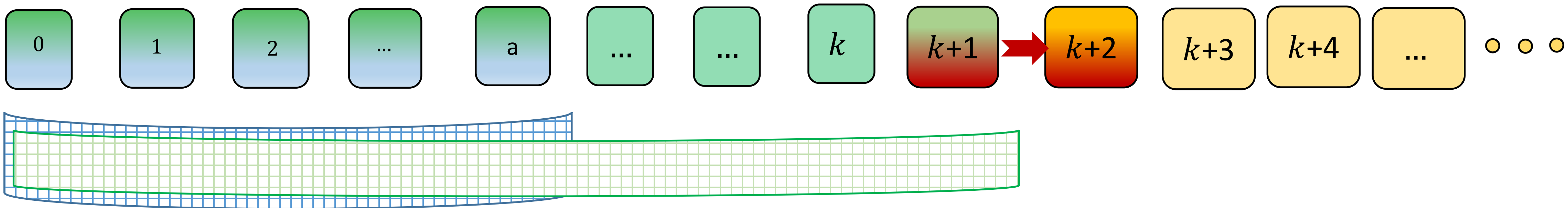
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \ldots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…



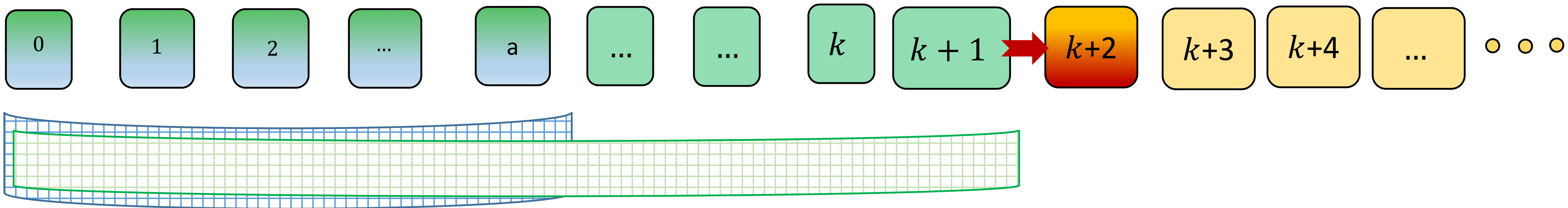
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \wedge P(k+1) \Longrightarrow P(k+2)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…



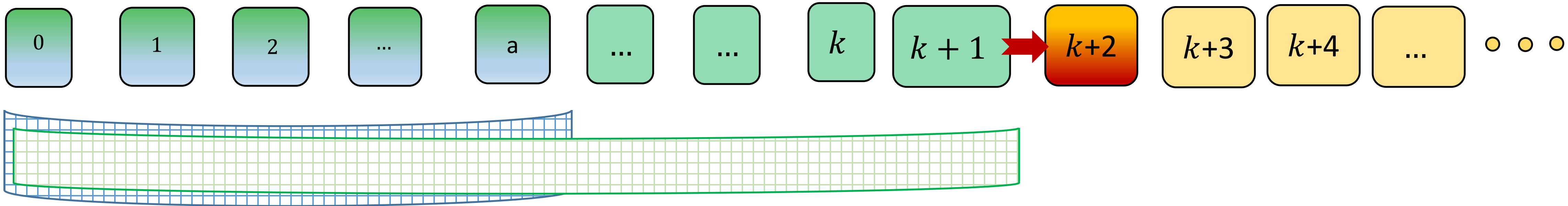
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  - *a)* $P(0), P(1), \dots, P(a)$ are true
  - b) For $n = k \geq a$,
    $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \wedge P(k+1) \Longrightarrow P(k+2)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…



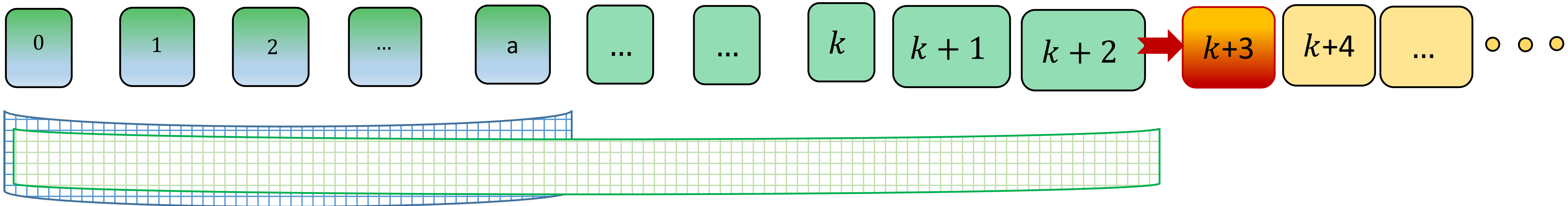
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  - *a)* $P(0), P(1), \dots, P(a)$ are true
  - b) For $n = k \geq a$,
    $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k) \wedge P(k+1) \Longrightarrow P(k+2)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…
  - And $P(k+3)$ …



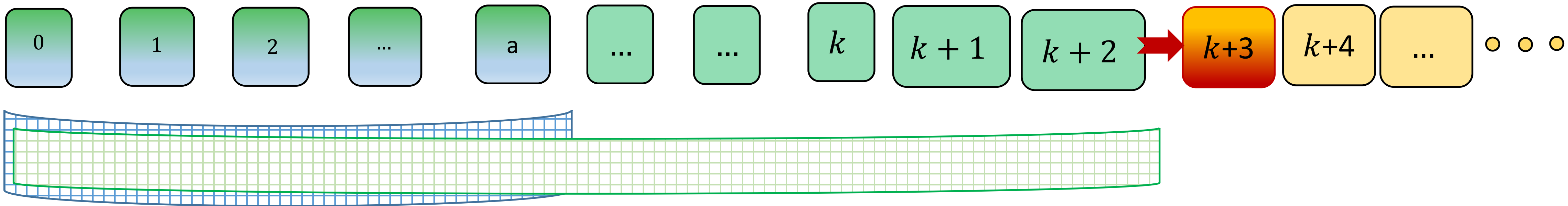
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
  $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k+1) \wedge P(k+2) \Longrightarrow P(k+3)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…
  - And $P(k+3)$ …



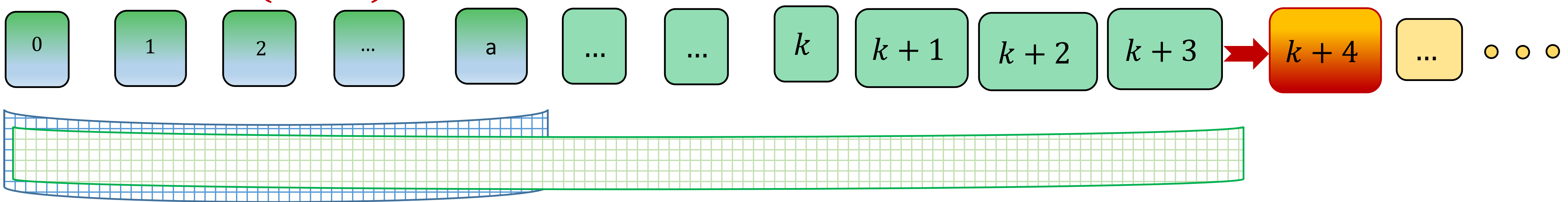
Strong Induction: The principle

- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \dots, P(a)$ are true
  b) For $n = k \geq a$,
     $\boldsymbol{P(0) \land P(1) \land \cdots \land P(a) \land P(a+1) \land \cdots \land P(k+1) \land P(k+2) \Longrightarrow P(k+3)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…
  - And $P(k+3)$ …
  - And $P(k+4)$ …



Strong Induction: The principle

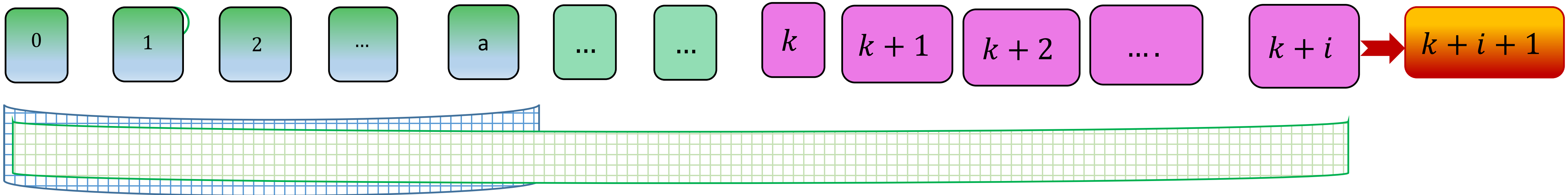
- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  a) $P(0), P(1), \ldots, P(a)$ are true
  b) For $n = k \geq a$,
  $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k+2) \wedge P(k+3) \Longrightarrow P(k+4)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$…
  - And $P(k+3)$ …
  - And $P(k+4)$ …



Strong Induction: The principle

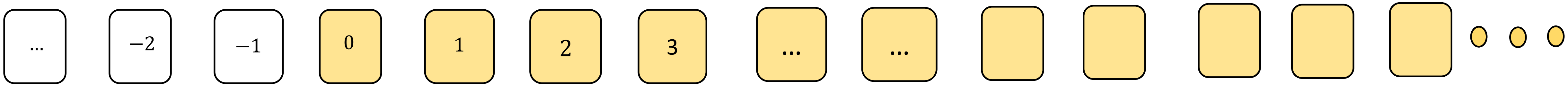
- The goal is the same: We want to prove a statement $P(n)\ \forall n \geq 0$
- The principle has, once again, two presuppositions. ***If:***
  - *a)* $P(0), P(1), \ldots, P(a)$ are true
  - b) For $n = k \geq a$,
    $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(a) \wedge P(a+1) \wedge \cdots \wedge P(k+2) \wedge P(k+3) \Longrightarrow P(k+4)}$
- ***Then***, $P(k+1)$ is also true
  - But then, so is $P(k+2)$, since we can simply **expand the net to include** $P(k+1)$...
  - And $P(k+3)$ ...
  - And $P(k+4)$ ...

And, generally, all $(k+i)$ ☺



How we'll make it work

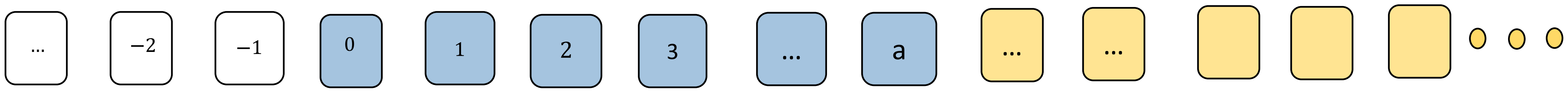
- We want to prove a statement $P(n)\ \forall n \geq 0$



How we'll make it work

1. **Inductive base:** We will **explicitly prove** (no matter how easy it might initially seem) that

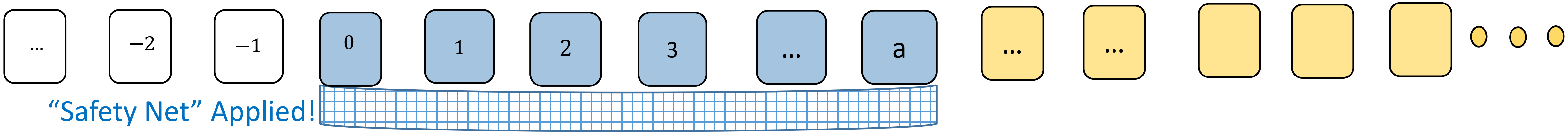
$$P(0), P(1), P(2), \dots, P(a)$$



How we'll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

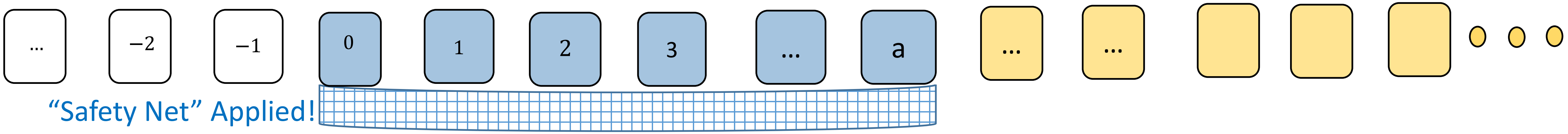


How we’ll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds

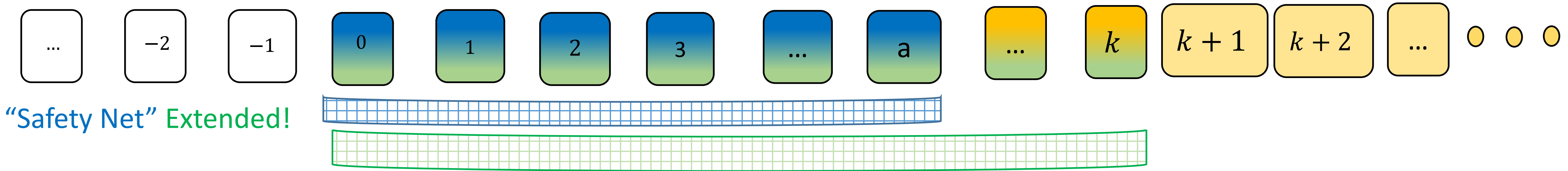


How we'll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \ldots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds

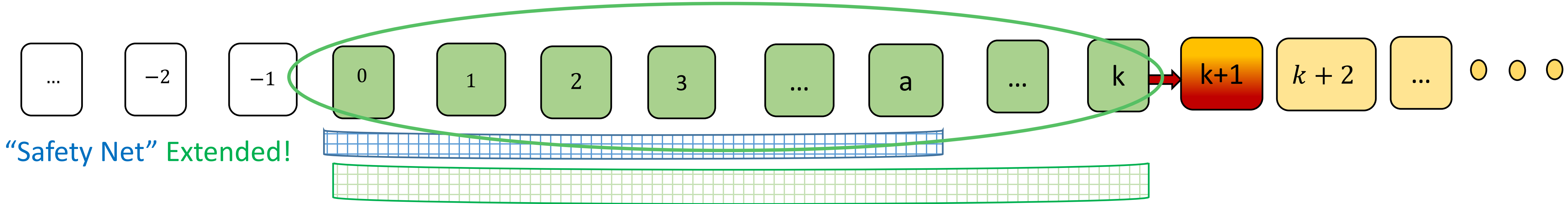


How we'll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds
3. Inductive step: We attempt to ***prove*** $P(k+1)$.



How we’ll make it work

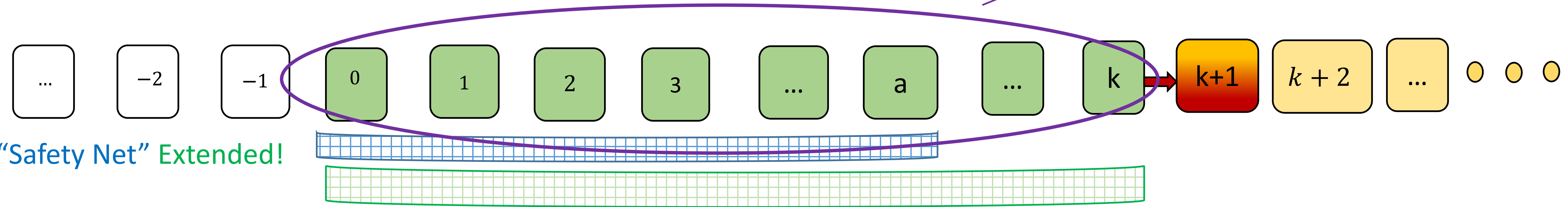
1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds

3. Inductive step: We attempt to ***prove*** $P(k+1)$.

Note that we assume $\boldsymbol{P(0) \wedge P(1) \wedge \cdots \wedge P(k)}$!



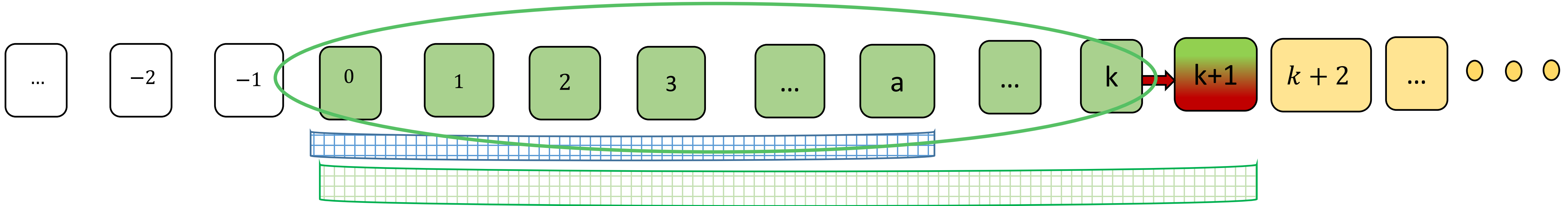
“Safety Net” Extended!

How we'll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds
3. Inductive step: We attempt to ***prove*** $P(k+1)$.
   - But, by the inductive principle, this means that we can expand our net some more…

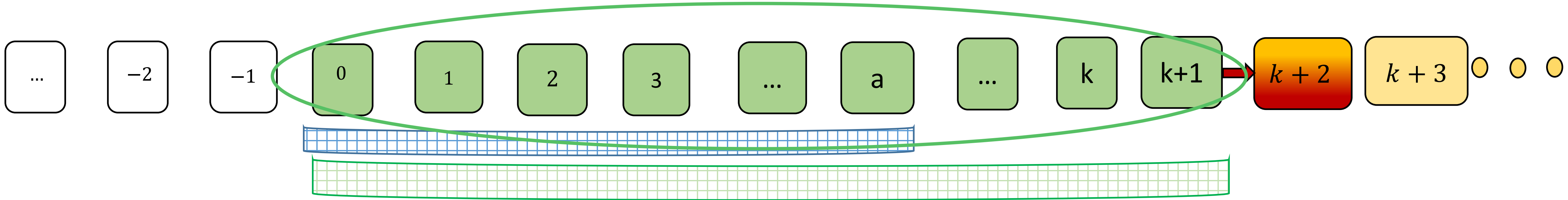


How we'll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds
3. Inductive step: We attempt to ***prove*** $P(k+1)$.
   - But, by the inductive principle, this means that we can expand our net some more…
   - And prove the statement for $k + 2$

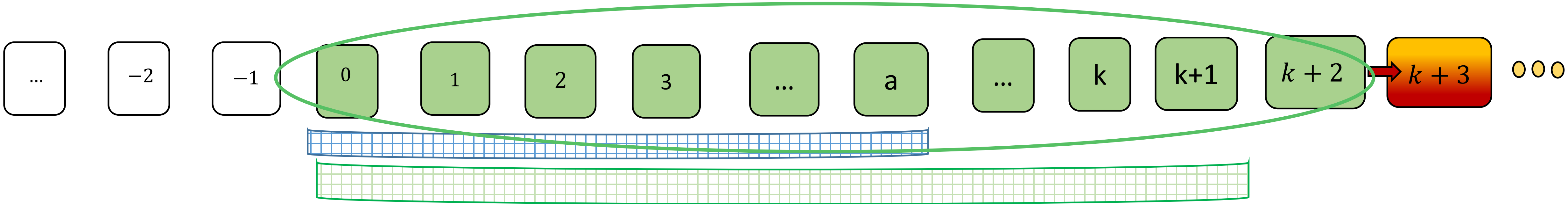


How we’ll make it work

1. **Inductive base:** We will ***explicitly prove*** (no matter how easy it might initially seem) that

$$P(0), P(1), P(2), \dots, P(a)$$

2. Inductive hypothesis: For $n = k \geq a$ and ***for every*** $i: 0 \leq i \leq k$, we will ***assume*** that $P(i)$ holds
3. Inductive step: We attempt to ***prove*** $P(k+1)$.
   - But, by the inductive principle, this means that we can expand our net some more…
   - And prove the statement for $k+2, k+3, \dots$



Utility of strong induction

- Enormous
  - Correctness of algorithms
  - Growth of structures like trees, graphs, lists, strings, sets

Utility of strong induction

- Enormous
  - Correctness of algorithms
  - Growth of structures like trees, graphs, lists, strings, sets
- **Terrifically** useful in sequences
  - How many ways have we talked about that can be used to describe a sequence?

1	2	3	4

Utility of strong induction

- Enormous
  - Correctness of algorithms
  - Growth of structures like trees, graphs, lists, strings, sets
- **Terrifically** useful in sequences
  - How many ways have we talked about that can be used to describe a sequence?

1 2 3 4

1. Outlining terms
2. Recursive definition
3. Closed-form formula

- Also useful in the study of **algorithm <u>correctness.</u>**

A first example

- Let a be a sequence such that:

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

- Prove that $a_n = 3 \cdot 2^n + 2(-1)^{n+1} \ , n \in \mathbb{N}$

A first example

- Let a be a sequence such that:

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

- Prove that $\underbrace{a_n = 3 \cdot 2^n + 2(-1)^{n+1}}_{P(n)}$ $, n \in \mathbb{N}$

- How many elements in my inductive base?

1

2

3

Something Else

A first example

- Let a be a sequence such that:

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

- Prove that $\underbrace{a_n = 3 \cdot 2^n + 2(-1)^{n+1}}_{P(n)}$ $, n \in \mathbb{N}$

- How many elements in my inductive base?

1

2

3

Something Else

Inductive base

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

$$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$$

- For $n = 0$, $a_0 = 1$ by the definition of a. $P(0)$ says: $a_0 = 3 \cdot 2^0 + 2(-1)^1 = 3 - 2 = 1$.
  So $P(0)$ holds.
- For n = 1, $a_1 = 8$ by the definition of a. $P(1)$ says: $a_1 = 3 \cdot 2^1 + 2(-1)^2 = 6 + 2 = 8$.

  So P(1) holds.

Inductive base

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$

- For $n = 0$, $a_0 = 1$ by the definition of a. $P(0)$ says: $a_0 = 3 \cdot 2^0 + 2(-1)^1 = 3 - 2 = 1$.
  So $P(0)$ holds.
- For n = 1, $a_1 = 8$ by the definition of a. $P(1)$ says: $a_1 = 3 \cdot 2^1 + 2(-1)^2 = 6 + 2 = 8$.

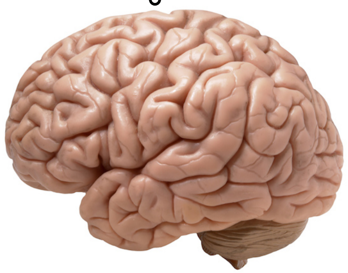
  So P(1) holds.

Inductive Base established!

Inductive Hypothesis

$P(\boxed{0})$ $P(\boxed{1})$

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$



$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$

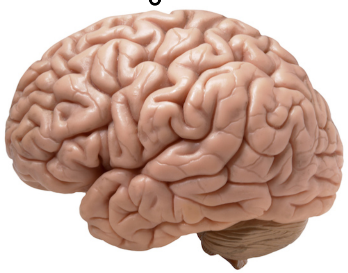
- Suppose $n = k \geq 1$. Then, $\forall i \in \{0, 1, \ \dots, k\}$ assume $P(i)$, i.e

$$a_i = 3 \cdot 2^i + 2(-1)^{i+1}, i = 0, 1, \dots, k$$

Inductive Hypothesis

$P(\boxed{0})\ \ P(\boxed{1})$

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$



$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$

- Suppose $n = k \geq 1$. Then, $\forall i \in \{0, 1, \ \ldots, k\}$ assume $P(i)$, i.e

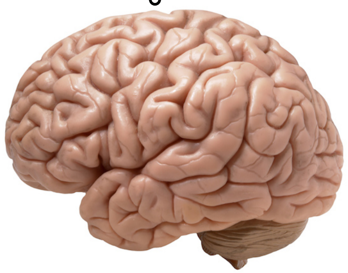
$$a_i = 3 \cdot 2^i + 2(-1)^{i+1}, i = 0, 1, \ldots, k$$

Inductive Hypothesis made!

Inductive Step

$P(\boxed{0})$ $P(\boxed{1})$

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$



$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$

$P(i)\ \forall i = 0,1, \ldots k$

- We will now **prove** $P(k+1)$, i.e

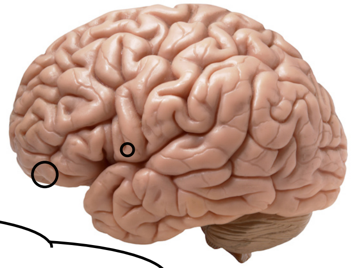
$$a_{k+1} = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$$

Inductive Step

$P(\boxed{0})$ $P(\boxed{1})$

$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$

$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$



$P(i)\ \forall i = 0,1,\ldots k$

My goal: Prove $P(k+1)$: $a_{k+1} = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$

- Since $\boldsymbol{k \geq 1 \Rightarrow (k+1) \geq 2}$, we can apply the recursive rule of the sequence.
- From the recursive definition of a_n, we obtain:

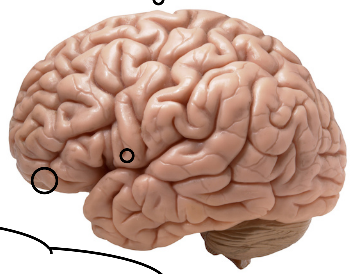
$$a_{k+1} = a_k + 2 \cdot a_{k-1} \overset{I.H}{=} 3 \cdot 2^k + 2(-1)^{k+1} + 2 \cdot \left(3 \cdot 2^{k-1} + 2\,(-1)^k\right) =$$
$$= 3 \cdot \left(2^k + 2 \cdot 2^{k-1}\right) + 2 \cdot (-1)^k[-1+2] =$$
$$= 3 \cdot \left(2 \cdot 2^k\right) + 2 \cdot (-1)^k = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$$

Inductive Step

$P(\boxed{0})$ $P(\boxed{1})$

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$



$P(i)\ \forall i = 0,1, \dots k$

My goal: Prove $P(k+1)$: $a_{k+1} = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$

- Since $\boldsymbol{k \geq 1 \Rightarrow (k+1) \geq 2}$, we can apply the recursive rule of the sequence.
- From the recursive definition of a_n, we obtain:

Inductive step proven!

$$a_{k+1} = a_k + 2 \cdot a_{k-1} \overset{I.H}{=} 3 \cdot 2^k + 2(-1)^{k+1} + 2 \cdot \left(3 \cdot 2^{k-1} + 2\,(-1)^k\right) =$$

$$= 3 \cdot \left(2^k + 2 \cdot 2^{k-1}\right) + 2 \cdot (-1)^k[-1+2] =$$

$$= 3 \cdot \left(2 \cdot 2^k\right) + 2 \cdot (-1)^k = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$$

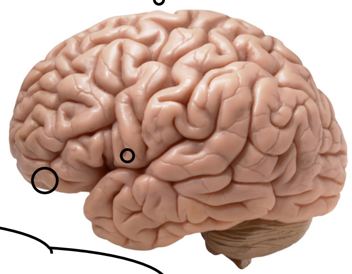
$\square$

Inductive Step

$P(\boxed{0})\quad P(\boxed{1})$

$$a_n = \begin{cases} 1, & n = 0 \\ 8, & n = 1 \\ a_{n-1} + 2 \cdot a_{n-2}, & n \geq 2 \end{cases}$$

$P(n) \Leftrightarrow a_n = 3 \cdot 2^n + 2(-1)^{n+1}$



$P(i)\ \forall i = 0,1,\dots k$

My goal: Prove $P(k+1)\colon\ a_{k+1} = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$

- Since $\boldsymbol{k \geq 1 \Rightarrow (k+1) \geq 2}$, we can apply the recursive rule of the sequence.
- From the recursive definition of a_n, we obtain:

$$a_{k+1} = a_k + 2 \cdot a_{k-1} \overset{I.H}{=} 3 \cdot 2^k + 2(-1)^{k+1} + 2 \cdot \left(3 \cdot 2^{k-1} + 2\,(-1)^k\right) =$$
$$= 3 \cdot \left(2^k + 2 \cdot 2^{k-1}\right) + 2 \cdot (-1)^k[-1+2] =$$
$$= 3 \cdot \left(2 \cdot 2^k\right) + 2 \cdot (-1)^k = 3 \cdot 2^{k+1} + 2(-1)^{k+2}$$

Proof done!

$\square$

Here's another

- Suppose that the sequence a_n is as follows:

$$a_n = \begin{cases} 12, & n = 0 \\ 29, & n = 1 \\ 5a_{n-1} - 6a_{n-2}, & n \geq 2 \end{cases}$$

- Then, prove that $a_n = 5 \cdot 3^n + 7 \cdot 2^n, \forall n \in \mathbb{N}$

Inductive base

- Let the statement to be proven be called $P(n)$. We proceed via strong induction on n.
- **Inductive base:** We want to ***prove*** $P(0), P(1)$.
  - For $n = 0, P(0)$ is $s_0 = 5 \cdot 3^0 + 7 \cdot 2^0 \Leftrightarrow 12 = 12$
  - For $n = 1, P(1)$ is $s_1 = 5 \cdot 3^1 + 7 \cdot 2^1 \Leftrightarrow 29 = 15 + 14$

So the inductive base has been established!

Inductive hypothesis

- Inductive Hypothesis: Let $n = k \geq 1$. Then, we ***assume*** that, **for all** $i = 0,1, \dots, k, P(i)$ holds, i.e

$$a_i = 5 \cdot 3^i + 7 \cdot 2^i, \quad i = 0,1, \dots, k$$

Inductive Step

- Inductive Step: We will attempt to ***prove*** $P(k+1)$, i.e

$$a_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$$

Inductive Step

- Inductive Step: We will attempt to ***prove*** $P(k+1)$, i.e

$$a_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$$

- Since $(k \geq 1), (k+1 \geq 2)$ and we can use the recursive definition of a.
- From the recursive definition of a we have:

$$a_{k+1} = 5a_k - 6a_{k-1} \overset{I.H}{=} 5\left(5 \cdot 3^k + 7 \cdot 2^k\right) - 6\left(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}\right)$$
$$= 25 \cdot 3^k + 35 \cdot 2^k - 30 \cdot 3^{k-1} - 42 \cdot 2^{k-1}$$
$$= 5 \cdot \left(5 \cdot 3^k - 2 \cdot 3^k\right) + 7\left(5 \cdot 2^k - 3 \cdot 2^k\right) = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1} \quad \square$$

Inductive Step

- Inductive Step: We will attempt to ***prove*** $P(k+1)$, i.e

$$a_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$$

- Since $(k \geq 1), (k+1 \geq 2)$ and we can use the recursive definition of a.
- From the recursive definition of a we have:

$$a_{k+1} = 5a_k - 6a_{k-1} \overset{I.H}{=} 5\left(5 \cdot 3^k + 7 \cdot 2^k\right) - 6\left(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}\right)$$
$$= 25 \cdot 3^k + 35 \cdot 2^k - 30 \cdot 3^{k-1} - 42 \cdot 2^{k-1}$$
$$= \underbrace{5 \cdot \left(5 \cdot 3^k - 2 \cdot 3^k\right) + 7\left(5 \cdot 2^k - 3 \cdot 2^k\right)}_{\text{Since we need factors of 5 and 7 in our result, we force them to appear and our lives automatically become easier!}} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1} \quad \square$$

A sequence problem for you!

- Let a_n be defined as:

$$a_n = \begin{cases} 5, & n = 0 \\ 16, & n = 1 \\ 7a_{n-1} - 10a_{n-2}, & n \geq 2 \end{cases}$$

- Prove that $a_n = 3 \cdot 2^n + 2 \cdot 5^n$

Existence part of UFT

- Recall the statement of UFT: For any integer $n \geq 2$, there exist unique $p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1}$ such that:

$$n = \prod_{i=0}^{r} p_i^{e_i}$$

- We will prove the existence part, i.e that

$$(\forall n \geq 2)(\exists p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1})[n = \prod_{i=0}^{r} p_i^{e_i}]$$

Existence part of UFT

- Recall the statement of UFT: For any integer $n \geq 2$, there exist unique $p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1}$ such that:

$$n = \prod_{i=0}^{r} p_i^{e_i}$$

- We will prove the existence part, i.e that

$$(\forall n \geq 2)(\exists p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1})[n = \prod_{i=0}^{r} p_i^{e_i}]$$

So it's an existential question, the affirmative of which we will prove ***constructively***, via induction!

Proof

- IB: For $n = 2$, $2 = 2^1$, so $(\exists p_1 \in \mathbf{P}, e_1 \in \mathbb{N}^{\geq 1})[2 = p_1^{e_1}]$. Done.
- I.H: Suppose $n = k \geq 2$. Then, assume that

$$(\forall j \in \{2, 3, \dots, k\})(\exists p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1})[k = \textstyle\prod_{i=0}^{r} p_i^{e_i}]$$

- I.S: We will now prove $P(k+1)$, i.e that

$$(\exists p_i' \in \mathbf{P}, e_i' \in \mathbb{N}^{\geq 1})\left[k + 1 = \prod_{i=0}^{r} {p_i'}^{e_i'}\right]$$

Proof

- IB: For $n = 2$, $2 = 2^1$, so $(\exists p_1 \in \mathbf{P}, e_1 \in \mathbb{N}^{\geq 1})[2 = p_1^{e_1}]$. Done.
- I.H: Suppose $n = k \geq 2$. Then, assume that

$$(\forall j \in \{2, 3, \dots, k\})(\exists p_i \in \mathbf{P}, e_i \in \mathbb{N}^{\geq 1})[k = \prod_{i=0}^{r} p_i^{e_i}]$$

- I.S: We will now prove $P(k+1)$, i.e that

$$(\exists p_i' \in \mathbf{P}, e_i' \in \mathbb{N}^{\geq 1})[k + 1 = \prod_{i=0}^{r} p_i'^{e_i'}]$$

- Case #1: $k + 1 \in \mathbf{P}$. Then, $p_1' = k + 1, e_1 = 1$. Done.
- Case #2: $k + 1 \notin \mathbf{P}$. Then, $(\exists \ell_1, \ell_2 \in \{2, 3, \dots, k\})[k + 1 = \ell_1 \cdot \ell_2]$

Inductive step contd. in next slide for readability…

Inductive step (contd.)

- Case #2: $k + 1 \notin \mathbf{P}$. Then, $(\exists \ell_1, \ell_2 \in \{2, 3, \ldots, k\})[k + 1 = \ell_1 \cdot \ell_2]$

Inductive step (contd.)

- Case #2: $k+1 \notin \mathbf{P}$. Then, $(\exists \ell_1, \ell_2 \in \{2, 3, \dots, k\})[k+1 = \ell_1 \cdot \ell_2]$
- By the Inductive Hypothesis,

$$(\exists q_i \in \mathbf{P}, s_i \in \mathbb{N}^{\geq 1})[\ell_1 = \prod_{i=0}^{m_1} q_i^{e_i}]$$

and

$$(\exists q_i' \in \mathbf{P}, s_i' \in \mathbb{N}^{\geq 1})[\ell_2 = \prod_{i=0}^{m_2} {q'}_i^{e_i'}]$$

Inductive step (contd.)

- Case #2: $k+1 \notin \mathbf{P}$. Then, $(\exists \ell_1, \ell_2 \in \{2, 3, \dots, k\})[k+1 = \ell_1 \cdot \ell_2]$
- By the Inductive Hypothesis,

$$(\exists q_i \in \mathbf{P}, s_i \in \mathbb{N}^{\geq 1})[\ell_1 = \prod_{i=0}^{m_1} q_i^{e_i}]$$

and

$$(\exists q_i' \in \mathbf{P}, s_i' \in \mathbb{N}^{\geq 1})[\ell_2 = \prod_{i=0}^{m_2} {q'}_i^{e_i'}]$$

- Therefore,

$$k+1 = \prod_{i=0}^{\max\{m_1, m_2\}} q_i^{e_i} \cdot {q'}_i^{e_i'}$$

which is a unique product of prime powers. Done.

Important note

- Recall case #2: $k + 1 \notin \mathbf{P}$. Then, $(\exists \ell_1, \ell_2 \in \{2, 3, \dots, k\})[k + 1 = \ell_1 \cdot \ell_2]$
- Note that $P(k + 1)$ depends on falling back to the assumed $P(\ell_1), P(\ell_2)$.

Important note

- In our proofs on recurrences, $P(k+1)$ dependent on stuff such as

$$P(k), P(k-1), P(k-2), \ldots$$

- It is possible (and common) for $P(k+1)$ to depend on

$$P\left({}^{(k+1)}/_{2}\right), P\left({}^{(k+1)}/_{3}\right), P(\sqrt{k+1}) \ldots$$

- Example: Case #2 of existence part of UPFT depends on two integers ℓ_1, ℓ_2 whose product is $k+1$
  - It must be the case that $2 \leq \ell_1, \ell_2 \leq \left\lfloor\sqrt{k+1}\right\rfloor \leq k$

Important note

- In our proofs on recurrences, $P(k+1)$ dependent on stuff such as

$$P(k), P(k-1), P(k-2), \ldots$$

- It is possible (and common) for $P(k+1)$ to depend on

$$P\left({}^{(k+1)}/_{2}\right), P\left({}^{(k+1)}/_{3}\right), P\left(\sqrt{k+1}\right) \ldots$$

- Example: Case #2 of existence part of UPFT depends on two integers ℓ_1, ℓ_2 whose product is $k+1$
  - It must be the case that $2 \leq \ell_1, \ell_2 \leq \left\lfloor \sqrt{k+1} \right\rfloor \leq k < k+1$