Generalization of proofs and codification of graph families

Lorenzo Sauras-Altuzarra

TU Wien

8ECM

Contents

Fermat numbers

- n-th Fermat number: $F(n) := 2^{2^n} + 1$.

Fermat numbers

- n-th Fermat number: $F(n) := 2^{2^n} + 1$.
- Only $F(0)$, ..., $F(11)$ are fully factored.

Fermat numbers

- n-th Fermat number: $F(n) := 2^{2^n} + 1$.
- Only $F(0)$, ..., $F(11)$ are fully factored.
- $F(20)$ and $F(24)$ are known to be composite, but no prime factor is known.

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641}$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \qquad \to \qquad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1)$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$$(*)\ x + 1 \mid x^4 - 1$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \to \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$$\searrow \qquad \swarrow$$

$$641 \mid 2^{32} + 1$$

$$(*) \ x + 1 \mid x^4 - 1$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$a_0 \mid b_0$

$\swarrow$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$\searrow$ $\swarrow$

$$641 \mid 2^{32} + 1$$

$$(*)\ x + 1 \mid x^4 - 1$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$a_0 \mid b_0$

$\swarrow$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1)$$

$$\underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$c_0 \mid d_0$

$\searrow \qquad \swarrow$

$$641 \mid 2^{32} + 1$$

$(*)$ $x + 1 \mid x^4 - 1$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \qquad \rightarrow \qquad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$a_0 \mid b_0 \;,\; a_1 \mid b_1 + c_1 \qquad\qquad a_1 \mid b_1 \cdot d_1 + c_1 \cdot d_1$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad\qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$$c_0 \mid d_0$$

$$\searrow \qquad\qquad \swarrow$$

$$641 \mid 2^{32} + 1$$

$$(*)\ x + 1 \mid x^4 - 1$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$a_0 \mid b_0 \;,\; a_1 \mid b_1 + c_1 \qquad a_1 \mid b_1 \cdot d_1 + c_1 \cdot d_1 \;,\; a_2 \mid b_2 + c_2$$

$\swarrow$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$$a_2 \mid (b_2 - d_2) + (c_2 + d_2) \qquad c_0 \mid d_0$$

$\searrow \qquad \swarrow$

$$641 \mid 2^{32} + 1$$

$(*)$ $x + 1 \mid x^4 - 1$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$a_0 \mid b_0 \;,\; a_1 \mid b_1 + c_1 \qquad a_1 \mid b_1 \cdot d_1 + c_1 \cdot d_1 \;,\; a_2 \mid b_2 + c_2$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \; (*)$$

$$a_2 \mid (b_2 - d_2) + (c_2 + d_2) \;,\; a_3 \mid b_3 + c_3 \qquad c_0 \mid d_0 \;,\; a_3 \mid b_3$$

$$\searrow \qquad \swarrow$$

$$641 \mid 2^{32} + 1$$

$$a_3 \mid c_3$$

$$(*)\; x + 1 \mid x^4 - 1$$

Baaz's generalization method

Input: Bennet and Kraïtchik's proof of $641 \mid F(5)$.

$$641 \mid \underbrace{5^4 + 2^4}_{641} \quad \rightarrow \quad 641 \mid 5^4 \cdot 2^{28} + 2^{32}$$

$$a_0 \mid b_0 \ , \ a_1 \mid b_1 + c_1 \qquad a_1 \mid b_1 \cdot d_1 + c_1 \cdot d_1 \ , \ a_2 \mid b_2 + c_2$$

$$A \mid D + B \qquad A \mid D \cdot C + B \cdot C$$

$$\swarrow$$

$$641 \mid (5^4 \cdot 2^{28} - 1) + (2^{32} + 1) \qquad \underbrace{5 \cdot 2^7 + 1}_{641} \mid 5^4 \cdot 2^{28} - 1 \ (*)$$

$$a_2 \mid (b_2 - d_2) + (c_2 + d_2) \ , \ a_3 \mid b_3 + c_3 \qquad c_0 \mid d_0 \ , \ a_3 \mid b_3$$

$$A \mid (D \cdot C - E) + (B \cdot C + E) \qquad A \mid D \cdot C - E$$

$$\searrow \qquad \swarrow$$

$$641 \mid 2^{32} + 1$$

$$a_3 \mid c_3$$

$$A \mid B \cdot C + E$$

$(*)$ $x + 1 \mid x^4 - 1$

Application to Fermat numbers

- Original calculation: $\left\{ \begin{array}{l} 641 \mid 5^4 + 2^4 \\ 641 \mid 5^4 \cdot 2^{28} - 1 \end{array} \right. \Rightarrow 641 \mid 2^{32} + 1.$

Application to Fermat numbers

- Original calculation: $\left\{ \begin{array}{l} 641 \mid 5^4 + 2^4 \\ 641 \mid 5^4 \cdot 2^{28} - 1 \end{array} \right. \Rightarrow 641 \mid 2^{32} + 1.$
- Generalization: $\left\{ \begin{array}{l} A \mid D + B \\ A \mid D \cdot C - E \end{array} \right. \Rightarrow A \mid B \cdot C + E.$

Application to Fermat numbers

- Original calculation: $\begin{cases} 641 \mid 5^4 + 2^4 \\ 641 \mid 5^4 \cdot 2^{28} - 1 \end{cases} \Rightarrow 641 \mid 2^{32} + 1.$
- Generalization: $\begin{cases} A \mid D + B \\ A \mid D \cdot C - E \end{cases} \Rightarrow A \mid B \cdot C + E.$
- Particularization: $\boxed{k \cdot 2^s + 1 \mid k^{2 \cdot r} + 2^{2^n - 2 \cdot r \cdot s} \Rightarrow k \cdot 2^s + 1 \mid F(n)}$
  ($A = k \cdot 2^s + 1$, $B = 2^{2^n - 2 \cdot r \cdot s}$, $C = 2^{2 \cdot r \cdot s}$, $D = k^{2 \cdot r}$, $E = 1$).
  Note that, by varying r, we can make $k^{2 \cdot r} + 2^{2^n - 2 \cdot r \cdot s}$ way smaller than $F(n)$.

Application to Fermat numbers

- Original calculation: $\begin{cases} 641 \mid 5^4 + 2^4 \\ 641 \mid 5^4 \cdot 2^{28} - 1 \end{cases} \Rightarrow 641 \mid 2^{32} + 1.$
- Generalization: $\begin{cases} A \mid D + B \\ A \mid D \cdot C - E \end{cases} \Rightarrow A \mid B \cdot C + E.$
- Particularization: $\boxed{k \cdot 2^s + 1 \mid k^{2 \cdot r} + 2^{2^n - 2 \cdot r \cdot s} \Rightarrow k \cdot 2^s + 1 \mid F(n)}$
  $(A = k \cdot 2^s + 1,\ B = 2^{2^n - 2 \cdot r \cdot s},\ C = 2^{2 \cdot r \cdot s},\ D = k^{2 \cdot r},\ E = 1).$
  Note that, by varying r, we can make $k^{2 \cdot r} + 2^{2^n - 2 \cdot r \cdot s}$ way smaller than $F(n)$.
- Remark: this method can be applied in any area of mathematics.

Other results

- Result 1: $\boxed{\begin{cases} d \mid k \cdot 2^s \\ (k \cdot 2^s + 1) \cdot d^{2 \cdot t} - (k \cdot 2^s)^{2 \cdot t} + 1 = F(n) \end{cases} \Rightarrow \; k \cdot 2^s + 1 \mid F(n)}$.

Other results

- Result 1: $\boxed{\left\{\begin{array}{l} d \mid k \cdot 2^s \\ (k \cdot 2^s + 1) \cdot d^{2 \cdot t} - (k \cdot 2^s)^{2 \cdot t} + 1 = F(n) \end{array}\right. \Rightarrow\ k \cdot 2^s + 1 \mid F(n)}$.
- Result 2: $\boxed{(k \cdot 2^s + 1 - k^{2 \cdot q}) \cdot 2^{2 \cdot q \cdot s} + 1 = F(n) \ \Rightarrow\ k \cdot 2^s + 1 \mid F(n)}$.
  This theorem was obtained by Baaz in 1999.

Other results

- Result 1: $\left\{\begin{array}{l} d \mid k\cdot 2^s \\ (k\cdot 2^s+1)\cdot d^{2\cdot t}-(k\cdot 2^s)^{2\cdot t}+1=F(n) \end{array}\right. \Rightarrow\ k\cdot 2^s+1 \mid F(n)$.
- Result 2: $(k\cdot 2^s+1-k^{2\cdot q})\cdot 2^{2\cdot q\cdot s}+1=F(n)\ \Rightarrow\ k\cdot 2^s+1 \mid F(n)$.
  This theorem was obtained by Baaz in 1999.
- Result 3: $p \mid (F(n-1)-1-p\cdot c)^2+1\ \Rightarrow\ p \mid F(n)$.
  Note that, by varying c, we can make $(F(n-1)-1-p\cdot c)^2+1$ way smaller than $F(n)$.

Other results

- Result 1: $\boxed{\begin{cases} d \mid k \cdot 2^s \\ (k \cdot 2^s + 1) \cdot d^{2 \cdot t} - (k \cdot 2^s)^{2 \cdot t} + 1 = F(n) \end{cases} \Rightarrow\ k \cdot 2^s + 1 \mid F(n)}$.
- Result 2: $\boxed{(k \cdot 2^s + 1 - k^{2 \cdot q}) \cdot 2^{2 \cdot q \cdot s} + 1 = F(n) \ \Rightarrow\ k \cdot 2^s + 1 \mid F(n)}$.
  This theorem was obtained by Baaz in 1999.
- Result 3: $\boxed{p \mid (F(n-1) - 1 - p \cdot c)^2 + 1 \ \Rightarrow\ p \mid F(n)}$.
  Note that, by varying c, we can make $(F(n-1) - 1 - p \cdot c)^2 + 1$ way smaller than $F(n)$.
- Result 4: $\boxed{p \nmid \dfrac{(F(n+2) - 1)^k - 1}{F(n)} \ \Leftrightarrow\ p \mid F(n)}$,
  where p equals $k \cdot 2^{n+2} + 1$ and is prime.
  The converse implication was proved by Wang.

Contents

Vertex-by-vertex increasing graph sequences

- A sequence G of simple graphs is vertex-by-vertex increasing if and only if $V(G_n) = \{1, ..., n+1\}$ and $E(G_n) \subseteq E(G_{n+1})$.

The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_1	$\mathrm{adj}(G_1)$	
1 —— 2	$\begin{bmatrix} * & * \\ 1 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$

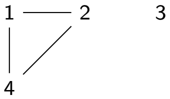
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_2	$\mathrm{adj}(G_2)$	
1 —— 2 3	$\begin{bmatrix} * & * & * \\ 1 & * & * \\ 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$

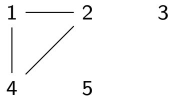
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_3	$\mathrm{adj}(G_3)$	
	$\begin{bmatrix} * & * & * & * \\ 1 & * & * & * \\ 0 & 0 & * & * \\ 1 & 1 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$

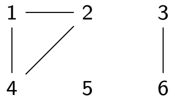
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

<table>
<tr><th>G_4</th><th>$\mathrm{adj}(G_4)$</th><th></th></tr>
<tr><td>
</td><td>$$\begin{bmatrix} * & * & * & * & * \\ 1 & * & * & * & * \\ 0 & 0 & * & * & * \\ 1 & 1 & 0 & * & * \\ 0 & 0 & 0 & 0 & * \end{bmatrix}$$</td><td>$(\Phi(G))_0 = 1$
$(\Phi(G))_1 = 0$
$(\Phi(G))_2 = 6$
$(\Phi(G))_3 = 0$</td></tr>
</table>

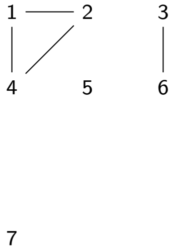
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_5	$\mathrm{adj}(G_5)$	
	$\begin{bmatrix} * & * & * & * & * & * \\ 1 & * & * & * & * & * \\ 0 & 0 & * & * & * & * \\ 1 & 1 & 0 & * & * & * \\ 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$ $(\Phi(G))_3 = 0$ $(\Phi(G))_4 = 4$

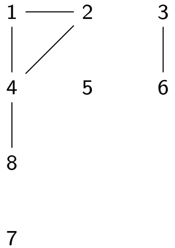
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_6	$\mathrm{adj}(G_6)$	
	$\begin{bmatrix} * & * & * & * & * & * & * \\ 1 & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * \\ 1 & 1 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 1 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$ $(\Phi(G))_3 = 0$ $(\Phi(G))_4 = 4$ $(\Phi(G))_5 = 0$

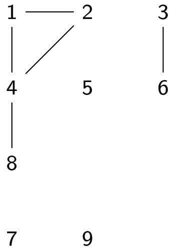
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_7	$\mathrm{adj}(G_7)$	
	$\begin{bmatrix} * & * & * & * & * & * & * & * \\ 1 & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * \\ 1 & 1 & 0 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 1 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$ $(\Phi(G))_3 = 0$ $(\Phi(G))_4 = 4$ $(\Phi(G))_5 = 0$ $(\Phi(G))_6 = 8$

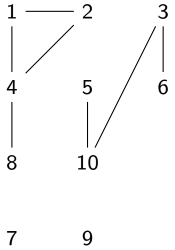
The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_8	$\mathrm{adj}(G_8)$	
	$\begin{bmatrix} * & * & * & * & * & * & * & * & * \\ 1 & * & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * & * \\ 1 & 1 & 0 & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * & * \\ 0 & 0 & 1 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$ $(\Phi(G))_3 = 0$ $(\Phi(G))_4 = 4$ $(\Phi(G))_5 = 0$ $(\Phi(G))_6 = 8$ $(\Phi(G))_7 = 0$

The bijection

Input: vertex-by-vertex increasing graph sequence G such that G_∞ is Collatz's graph.

G_9	$\mathrm{adj}(G_9)$	
	$\begin{bmatrix} * & * & * & * & * & * & * & * & * & * \\ 1 & * & * & * & * & * & * & * & * & * \\ 0 & 0 & * & * & * & * & * & * & * & * \\ 1 & 1 & 0 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & * & * & * & * & * & * \\ 0 & 0 & 1 & 0 & 0 & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & * & * & * & * \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & * \end{bmatrix}$	$(\Phi(G))_0 = 1$ $(\Phi(G))_1 = 0$ $(\Phi(G))_2 = 6$ $(\Phi(G))_3 = 0$ $(\Phi(G))_4 = 4$ $(\Phi(G))_5 = 0$ $(\Phi(G))_6 = 8$ $(\Phi(G))_7 = 0$ $(\Phi(G))_8 = 80$

Application to Collatz Problem

- Output: $(\Phi(G))_n = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ \sqrt{2^n} + \sqrt[3]{4^{n+1}}, & \text{if } n \in \{6 \cdot r + 2\}_{r \in \mathbb{N}}; \\ \sqrt{2^n}, & \text{otherwise,} \end{cases}$
  (first terms: 1, 0, 6, 0, 4, 0, 8, 0, 80...).

Application to Collatz Problem

- Output: $(\Phi(G))_n = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ \sqrt{2^n} + \sqrt[3]{4^{n+1}}, & \text{if } n \in \{6 \cdot r + 2\}_{r \in \mathbb{N}}; \\ \sqrt{2^n}, & \text{otherwise,} \end{cases}$
  (first terms: 1, 0, 6, 0, 4, 0, 8, 0, 80...).
- Collatz Problem: is G_∞ connected?

Application to Collatz Problem

- Output: $(\Phi(G))_n = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ \sqrt{2^n} + \sqrt[3]{4^{n+1}}, & \text{if } n \in \{6 \cdot r + 2\}_{r \in \mathbb{N}}; \\ \sqrt{2^n}, & \text{otherwise,} \end{cases}$
  (first terms: 1, 0, 6, 0, 4, 0, 8, 0, 80...).
- Collatz Problem: is G_∞ connected?
- Pattern observed: if $n \geq 3$, then the number of connected components of G_n is apparently $\left\lfloor \frac{n+2}{2} \right\rfloor - \left\lfloor \frac{n+3}{6} \right\rfloor + 1$.

Application to Collatz Problem

- Output: $(\Phi(G))_n = \begin{cases} 0, & \text{if } n \text{ is odd;} \\ \sqrt{2^n} + \sqrt[3]{4^{n+1}}, & \text{if } n \in \{6 \cdot r + 2\}_{r \in \mathbb{N}}; \\ \sqrt{2^n}, & \text{otherwise,} \end{cases}$
(first terms: 1, 0, 6, 0, 4, 0, 8, 0, 80...).
- Collatz Problem: is G_∞ connected?
- Pattern observed: if $n \geq 3$, then the number of connected components of G_n is apparently $\left\lfloor \frac{n+2}{2} \right\rfloor - \left\lfloor \frac{n+3}{6} \right\rfloor + 1$.
- Remark: because Φ is a bijection, we can input integer sequences instead (provided that they are upper-bounded by 2^{n+1}).