$0101 \oplus 1001 = 1100$

Andrzej Komisarski

andkom@math.uni.lodz.pl

Wydział Matematyki i Informatyki
Uniwersytet Łódzki

LIX Szkoła Matematyki Poglądowej
15 lutego 2019 r.
Wola Ducka

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

$$a \oplus b = \begin{cases} 0 & \text{gdy } a = b \\ 1 & \text{gdy } a \neq b \end{cases}$$

dla $a, b \in \{0, 1\}$

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

$$a \oplus b = \begin{cases} 0 & \text{gdy } a = b \\ 1 & \text{gdy } a \neq b \end{cases}$$

dla $a, b \in \{0, 1\}$

$a \oplus b$ to reszta z dzielenia $a + b$ przez 2

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

$$a \oplus b = \begin{cases} 0 & \text{gdy } a = b \\ 1 & \text{gdy } a \neq b \end{cases}$$

dla $a, b \in \{0, 1\}$

$a \oplus b$ to reszta z dzielenia $a + b$ przez 2

Działanie $\oplus$ jest łączne i przemienne
$(\{0, 1\}, \oplus)$ to grupa przemienna (ozn. $\mathbb{Z}_2$)

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

$$a \oplus b = \begin{cases} 0 & \text{gdy } a = b \\ 1 & \text{gdy } a \neq b \end{cases}$$

dla $a, b \in \{0, 1\}$

$a \oplus b$ to reszta z dzielenia $a + b$ przez 2

Działanie $\oplus$ jest łączne i przemienne
$(\{0, 1\}, \oplus)$ to grupa przemienna (ozn. $\mathbb{Z}_2$)

Ponadto $a \oplus 0 = 0 \oplus a = a$ oraz $a \oplus a = 0$

XOR, czyli $\oplus$, czyli dodawanie w $\mathbb{Z}_2$

XOR, czyli $\oplus$, to następujące działanie w zbiorze $\{0, 1\}$

$0 \oplus 0 = 0$
$0 \oplus 1 = 1$
$1 \oplus 0 = 1$
$1 \oplus 1 = 0$

$\oplus$	0	1
0	0	1
1	1	0

$$a \oplus b = \begin{cases} 0 & \text{gdy } a = b \\ 1 & \text{gdy } a \neq b \end{cases}$$

dla $a, b \in \{0, 1\}$

$a \oplus b$ to reszta z dzielenia $a + b$ przez 2

Działanie $\oplus$ jest łączne i przemienne
$(\{0, 1\}, \oplus)$ to grupa przemienna (ozn. $\mathbb{Z}_2$)

Ponadto $a \oplus 0 = 0 \oplus a = a$ oraz $a \oplus a = 0$

Jeśli $a_1, a_2, \ldots, a_n \in \{0, 1\}$, to $a_1 \oplus a_2 \oplus \cdots \oplus a_n =$
$=$ reszta z dzielenia $a_1 + a_2 + \cdots + a_n$ przez $2 =$

$$= \begin{cases} 0 & \text{gdy wśród } a_1, a_2, \ldots, a_n \text{ jest parzyście wiele jedynek} \\ 1 & \text{gdy wśród } a_1, a_2, \ldots, a_n \text{ jest nieparzyście wiele jedynek} \end{cases}$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$.

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Na przykład

$$77 \oplus 25 =$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Na przykład

$$77 \oplus 25 = 1001101_2 \oplus 0011001_2 =$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Na przykład

$$77 \oplus 25 = 1001101_2 \oplus 0011001_2 = 1010100_2 =$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Na przykład

$$77 \oplus 25 = 1001101_2 \oplus 0011001_2 = 1010100_2 = 84$$

XOR, czyli $\oplus$ w $\mathbb{Z}_2^k$ oraz w $\mathbb{Z}_+$

W potęgach $\{0,1\}^k$ działanie $\oplus$ określamy po współrzędnych (produktujemy grupy). Na przykład dla $k = 4$ mamy

$$0101 \oplus 1001 = 1100$$

$(\{0,1\}^k, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0 \ldots 0$.

Wykorzystując zapis binarny liczb całkowitych określamy $\oplus$ w $\mathbb{Z}_+ = \{0, 1, \ldots\}$. Na przykład

$$77 \oplus 25 = 1001101_2 \oplus 0011001_2 = 1010100_2 = 84$$

$(\mathbb{Z}_+, \oplus)$ jest grupą przemienną i dla każdego a zachodzi $a \oplus a = 0$.

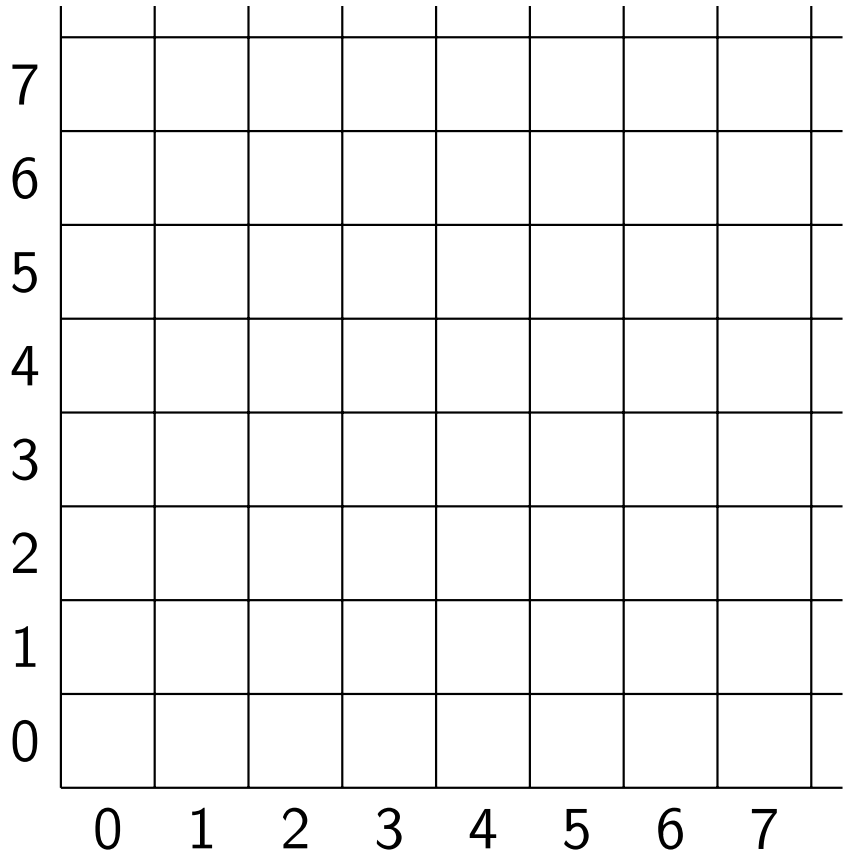
XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

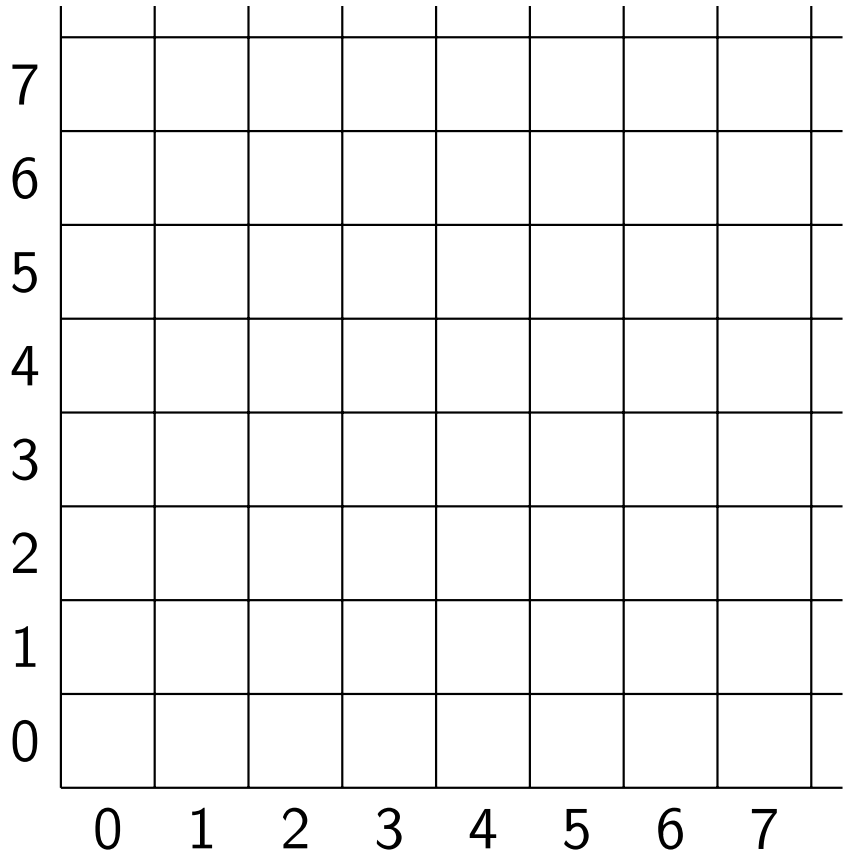


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

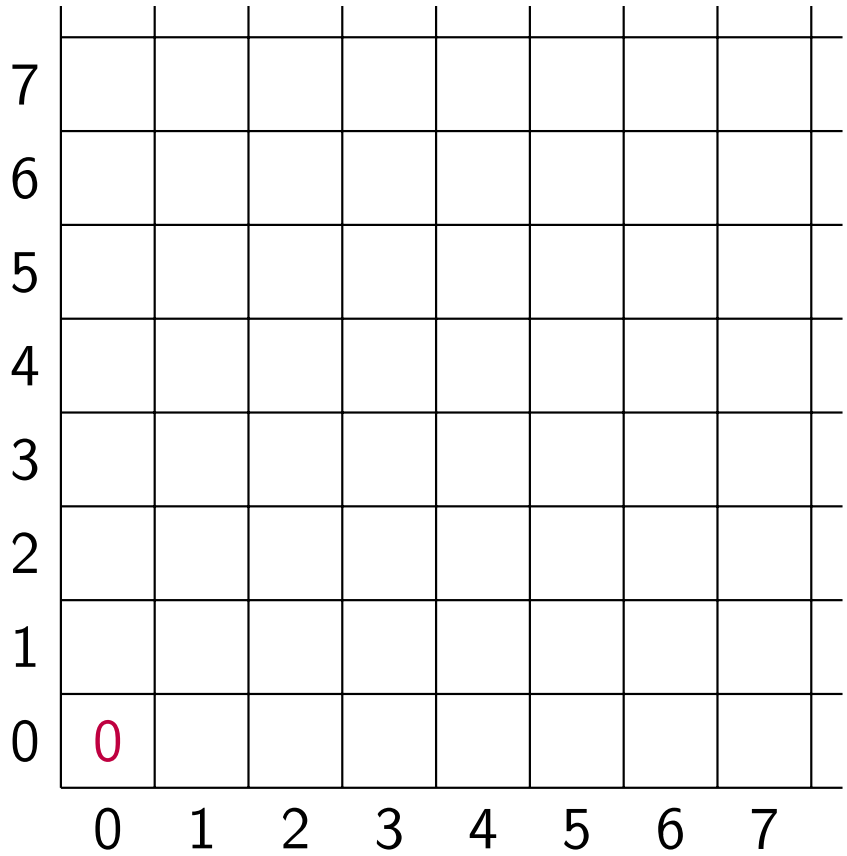


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

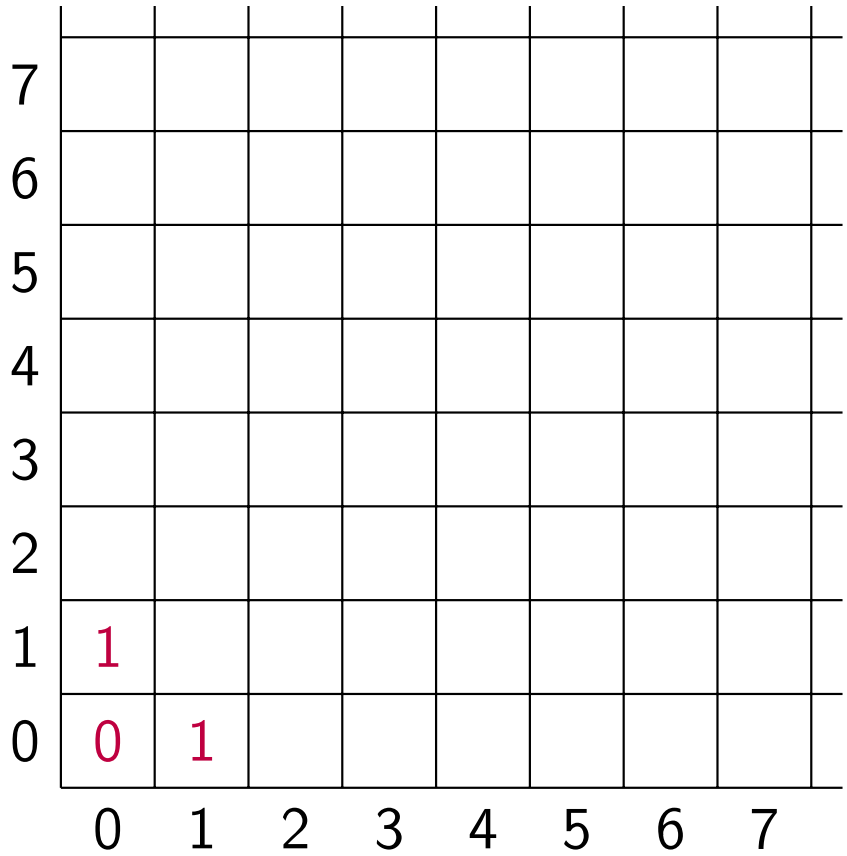


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

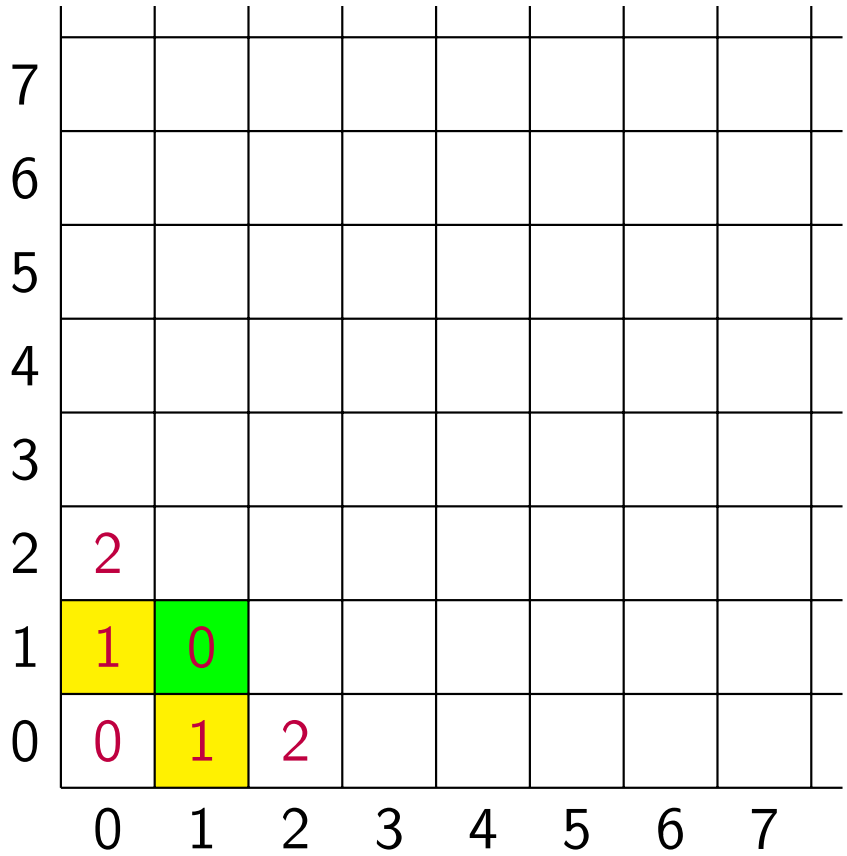


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

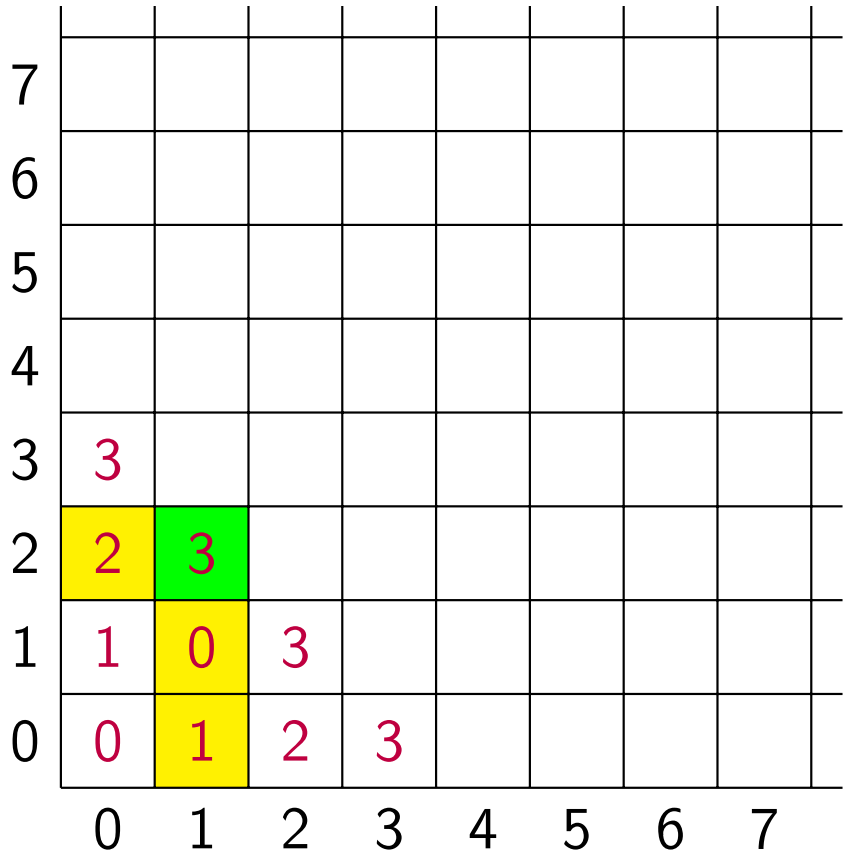


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

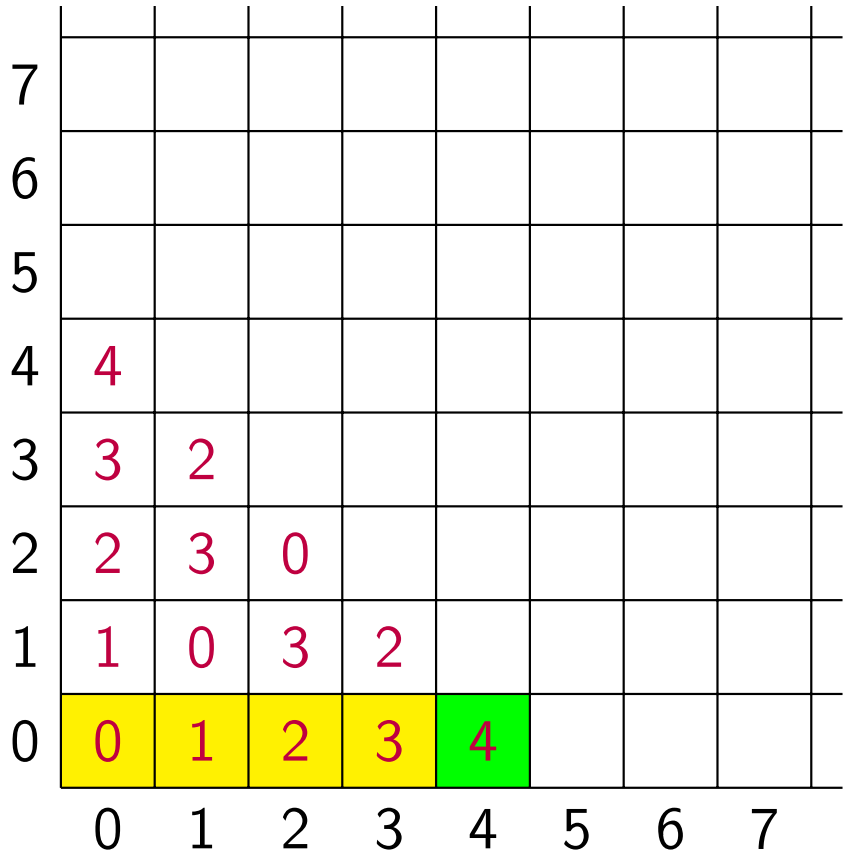


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

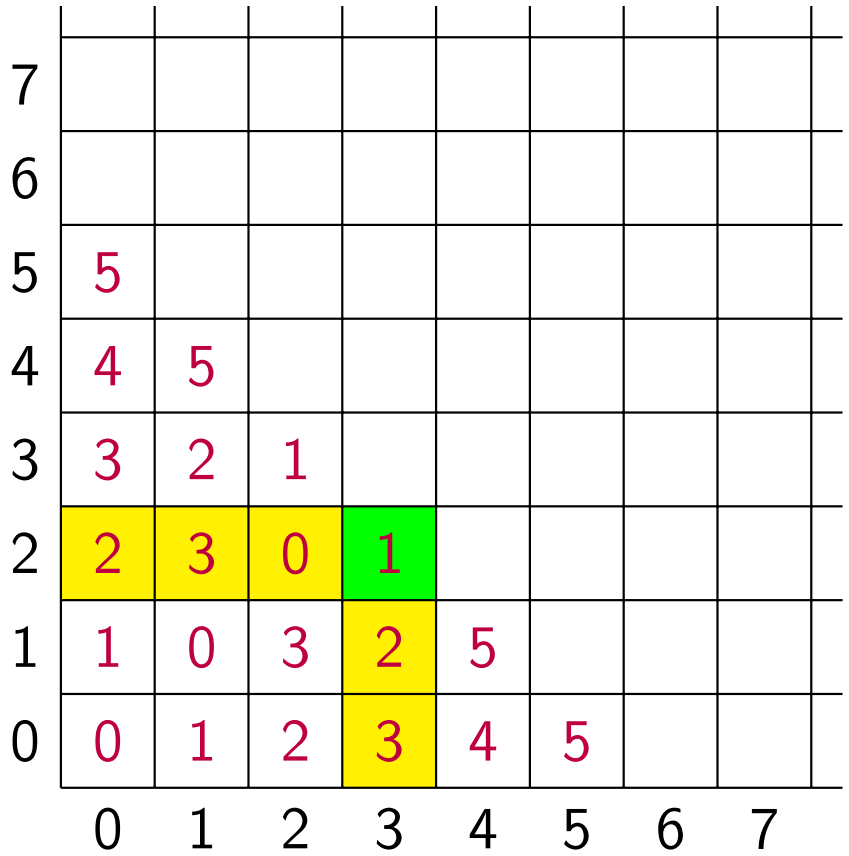


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

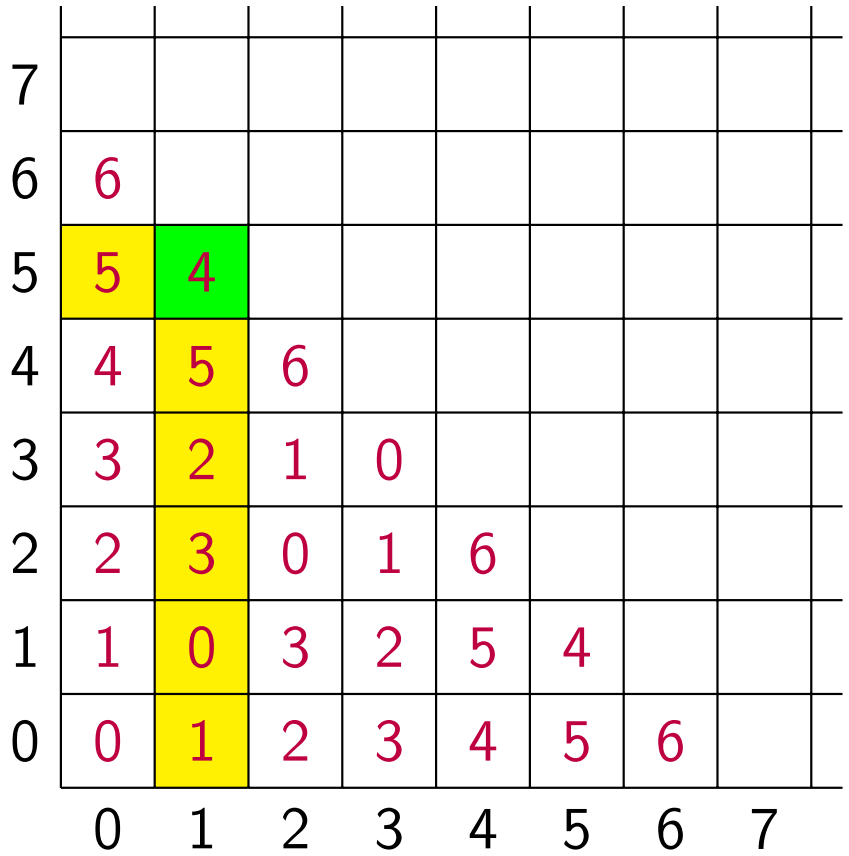


XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.



XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

7	7							
6	6	7						
5	5	4	7					
4	4	5	6	7				
3	3	2	1	0	7			
2	2	3	0	1	6	7		
1	1	0	3	2	5	4	7	
0	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

Okazuje się, że w polu o współrzędnych (i, j) wpisana zostanie liczba $i \oplus j$.

7	7	6	5	4	3	2	1	0
6	6	7	4	5	2	3	0	1
5	5	4	7	6	1	0	3	2
4	4	5	6	7	0	1	2	3
3	3	2	1	0	7	6	5	4
2	2	3	0	1	6	7	4	5
1	1	0	3	2	5	4	7	6
0	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

XOR, czyli $\oplus$ w $\mathbb{Z}_+$ bez systemu dwójkowego

Tak naprawdę $\oplus$ w $\mathbb{Z}_+$ ma mniej wspólnego z zapisem binarnym, niż się wydaje.

Rozważmy następującą tablicę:

W każde pole wpisujemy najmniejszą liczbę z $\mathbb{Z}_+ = \{0, 1, 2, \dots\}$, która nie jest wpisana w żadne pole poniżej, ani w żadne pole na lewo od danego pola.

Okazuje się, że w polu o współrzędnych (i, j) wpisana zostanie liczba $i \oplus j$.

7	7	6	5	4	3	2	1	0
6	6	7	4	5	2	3	0	1
5	5	4	7	6	1	0	3	2
4	4	5	6	7	0	1	2	3
3	3	2	1	0	7	6	5	4
2	2	3	0	1	6	7	4	5
1	1	0	3	2	5	4	7	6
0	0	1	2	3	4	5	6	7
	0	1	2	3	4	5	6	7

Jeśli $f : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ spełnia

$$f(i,j) = \min(\mathbb{Z}_+ \setminus (\{f(i,k) : k<j\} \cup \{f(l,j) : l<i\})),$$

to $f(i, j) = i \oplus j$.

Dlaczego? DIY

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n - 1\}$.
Jak to zrobić?

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n - 1\}$.
Jak to zrobić? Wysłać potajemnie SMSa!!!

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n - 1\}$.
Jak to zrobić? ~~Wysłać potajemnie SMSa!!!~~
Jedyne co możemy to odwrócić dokładnie jedną monetę. Którą?

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n - 1\}$.
Jak to zrobić? ~~Wysłać potajemnie SMSa!!!~~
Jedyne co możemy to odwrócić dokładnie jedną monetę. Którą?

Odwróćmy monetę o numerze $a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x$.

A co ma zrobić Magik?

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n - 1\}$.
Jak to zrobić? ~~Wysłać potajemnie SMSa!!!~~
Jedyne co możemy to odwrócić dokładnie jedną monetę. Którą?

Odwróćmy monetę o numerze $a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x$.

A co ma zrobić Magik?
Ma zXORować numery wszystkich monet, na których widzi orła.

Dlaczego to działa?

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n-1\}$.
Jak to zrobić? ~~Wysłać potajemnie SMSa!!!~~
Jedyne co możemy to odwrócić dokładnie jedną monetę. Którą?

Odwróćmy monetę o numerze $a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x$.

A co ma zrobić Magik?
Ma zXORować numery wszystkich monet, na których widzi orła.

Dlaczego to działa? Dlatego, że

$$a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus (a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x) =$$

$$= (a_1 \oplus a_1) \oplus (a_2 \oplus a_2) \oplus \cdots \oplus (a_j \oplus a_j) \oplus x = 0 \oplus 0 \oplus \cdots \oplus 0 \oplus x = x$$

Rozwiązanie zagadki z monetami

Mamy $n = 2^k$ monet.
Numerujemy je kolejnymi liczbami od 0 do $n - 1$.
Niektóre z nich $(a_1, a_2, \ldots, a_j)$ odwrócone są orłem do góry.
Mamy przekazać jakoś Magikowi liczbę $x \in \{0, 1, \ldots, n-1\}$.
Jak to zrobić? ~~Wysłać potajemnie SMSa!!!~~
Jedyne co możemy to odwrócić dokładnie jedną monetę. Którą?

Odwróćmy monetę o numerze $a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x$.

A co ma zrobić Magik?
Ma zXORować numery wszystkich monet, na których widzi orła.

Dlaczego to działa? Dlatego, że

$$a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus (a_1 \oplus a_2 \oplus \cdots \oplus a_j \oplus x) =$$

$$= (a_1 \oplus a_1) \oplus (a_2 \oplus a_2) \oplus \cdots \oplus (a_j \oplus a_j) \oplus x = 0 \oplus 0 \oplus \cdots \oplus 0 \oplus x = x$$

Ta metoda nie zadziała, gdy n nie jest potęgą dwójki. Nie zadziała też żadna inna. Dlaczego? DIY

Ratujmy krasnoludki! I

Dawno temu, jak wieść niesie,
W koniczyny gęstym lesie
Gdzieś przycupnął po cichutku
Domek czterech krasnoludków.

Krasnoludków czterech szereg
Idzie właśnie na spacerek.
Gęstym borem wśród konwalii
Idą wszyscy szukać malin.

[...]




Ratujmy krasnoludki! I

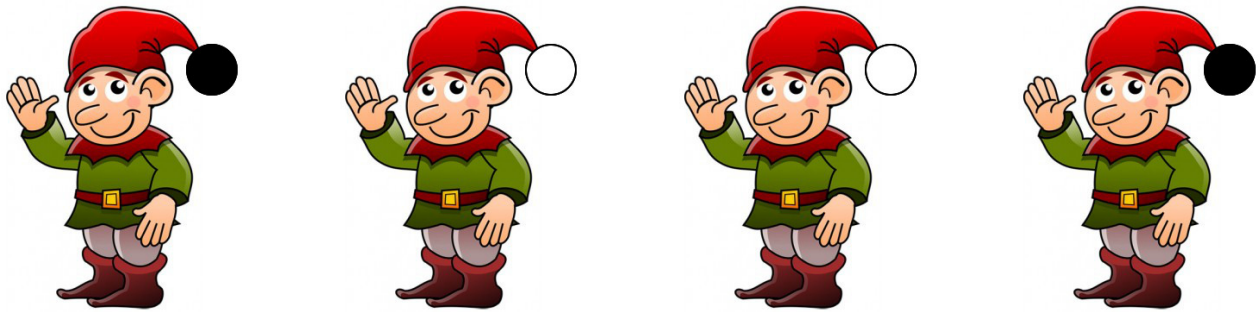
Dawno temu, jak wieść niesie,
W koniczyny gęstym lesie
Gdzieś przycupnął po cichutku
Domek czterech krasnoludków.

Krasnoludków czterech szereg
Idzie właśnie na spacerek.
Gęstym borem wśród konwalii
Idą wszyscy szukać malin.

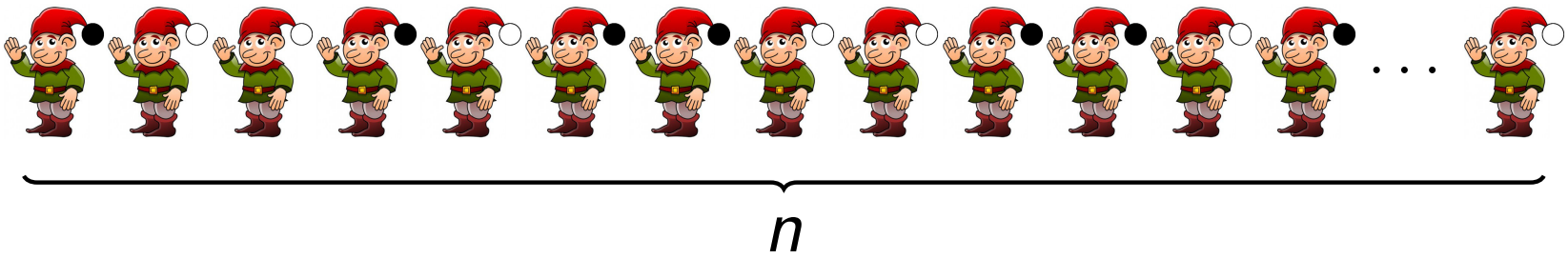
[...]



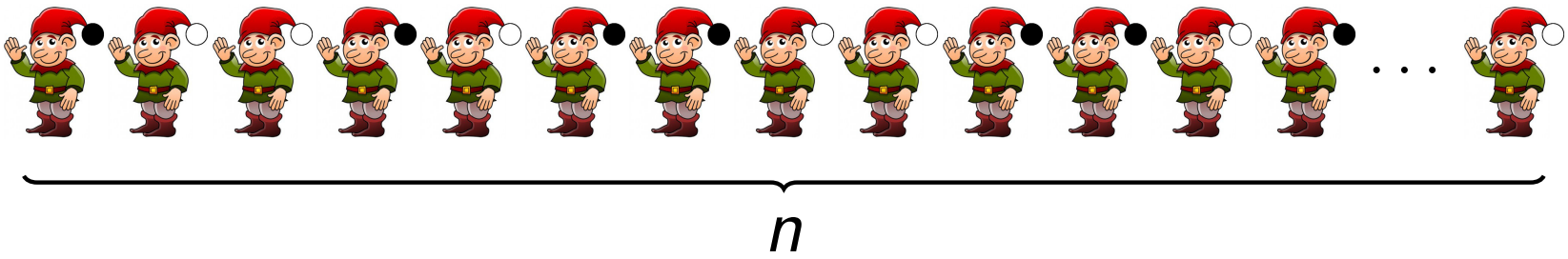

Krasnoludków czterech szereg idzie właśnie na spacerek.



Krasnoludków ~~czterech~~ n szereg idzie właśnie na spacerek.



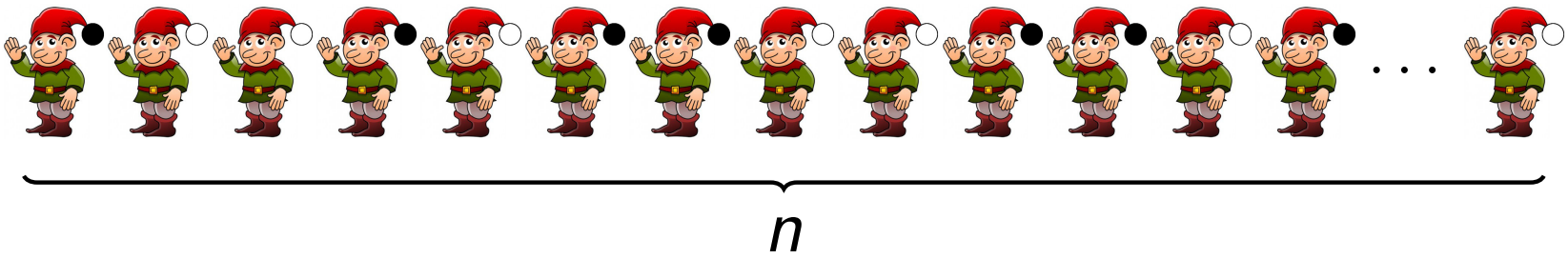
Krasnoludków ~~czterech~~ n szereg idzie właśnie na spacerek.



n

Bardzo zła i brzydka czarownica założyła krasnoludkom czapki z białymi lub czarnymi pomponami. Każdy krasnoludek widzi tylko kolory pomponów czapek wszystkich krasnoludków, którzy stoją w szeregu przed nim.

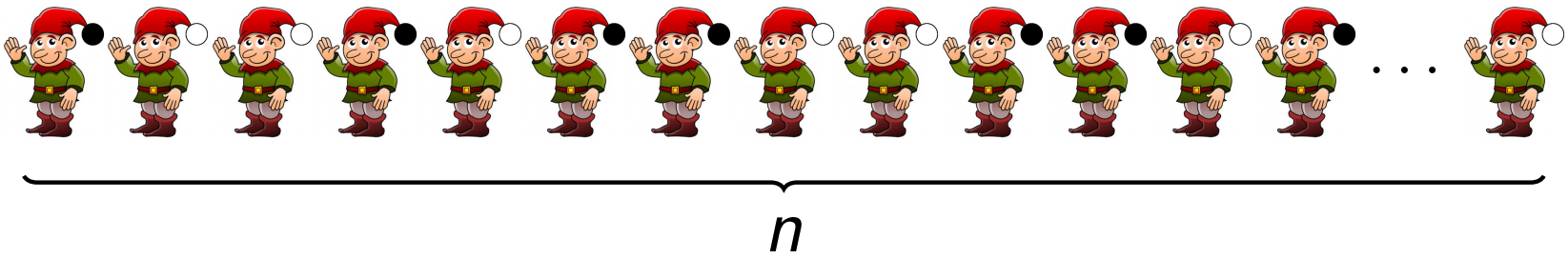
Krasnoludków ~~czterech~~ n szereg idzie właśnie na spacerek.



Bardzo zła i brzydka czarownica założyła krasnoludkom czapki z białymi lub czarnymi pomponami. Każdy krasnoludek widzi tylko kolory pomponów czapek wszystkich krasnoludków, którzy stoją w szeregu przed nim.

Począwszy od końca szeregu każdy krasnoludek ma podać jeden z dwóch kolorów (biały lub czarny). Wszystkie krasnoludki słyszą wszystkie odpowiedzi.

Krasnoludków ~~czterech~~ n szereg idzie właśnie na spacerek.

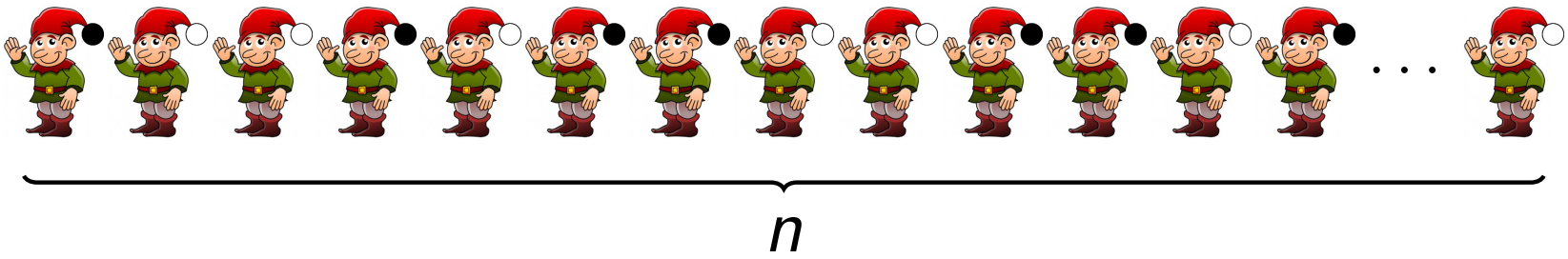


Bardzo zła i brzydka czarownica założyła krasnoludkom czapki z białymi lub czarnymi pomponami. Każdy krasnoludek widzi tylko kolory pomponów czapek wszystkich krasnoludków, którzy stoją w szeregu przed nim.

Począwszy od końca szeregu każdy krasnoludek ma podać jeden z dwóch kolorów (biały lub czarny). Wszystkie krasnoludki słyszą wszystkie odpowiedzi.

Te krasnoludki, które podały kolor inny, niż kolor swego pompona zostaną ugotowane i zjedzone przez złą (i bardzo brzydką) czarownicę.

Krasnoludków ~~czterech~~ n szereg idzie właśnie na spacerek.



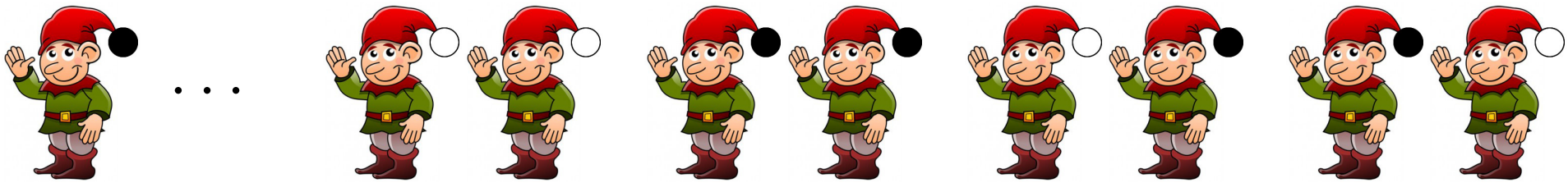
Bardzo zła i brzydka czarownica założyła krasnoludkom czapki z białymi lub czarnymi pomponami. Każdy krasnoludek widzi tylko kolory pomponów czapek wszystkich krasnoludków, którzy stoją w szeregu przed nim.

Począwszy od końca szeregu każdy krasnoludek ma podać jeden z dwóch kolorów (biały lub czarny). Wszystkie krasnoludki słyszą wszystkie odpowiedzi.

Te krasnoludki, które podały kolor inny, niż kolor swego pompona zostaną ugotowane i zjedzone przez złą (i bardzo brzydką) czarownicę.

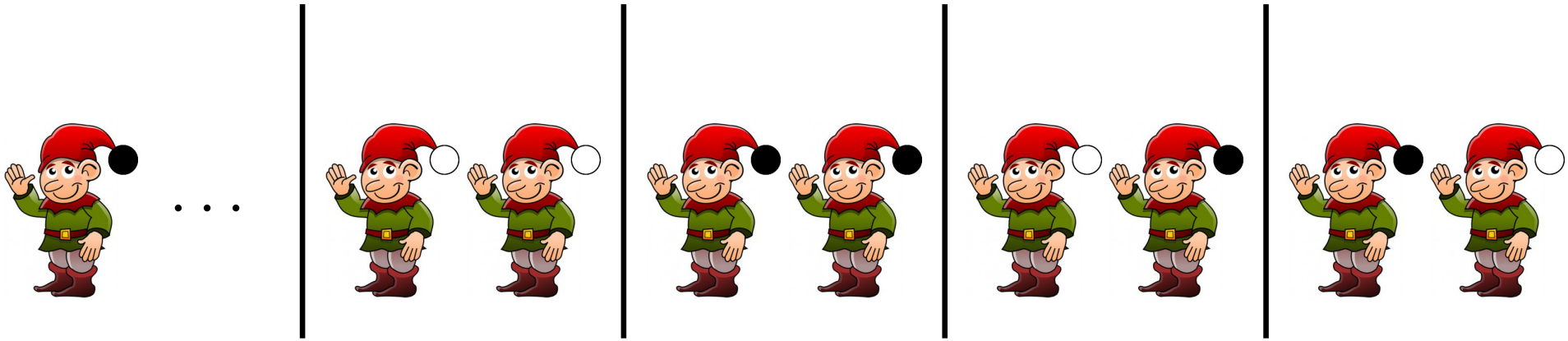
Pomóżmy krasnoludkom! Wymyślmy taką strategię, by możliwie wielu z nich uratowało się (nawet w pesymistycznym przypadku).

Strategia I



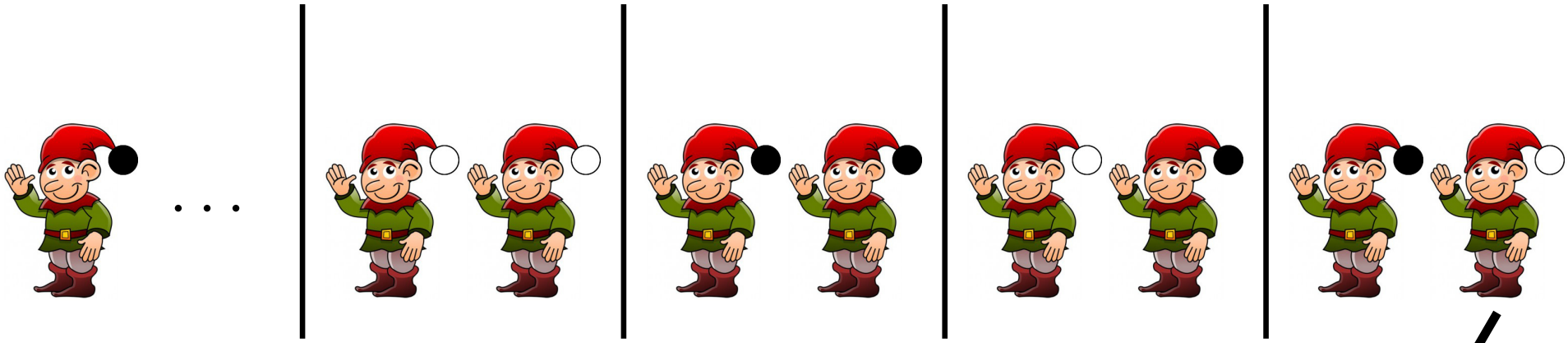
Strategia I

Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Strategia I

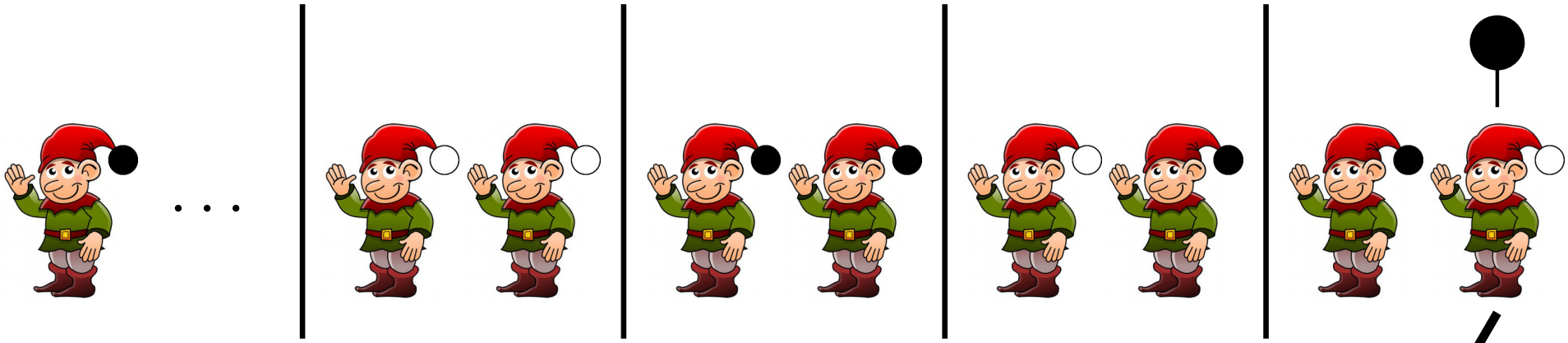
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

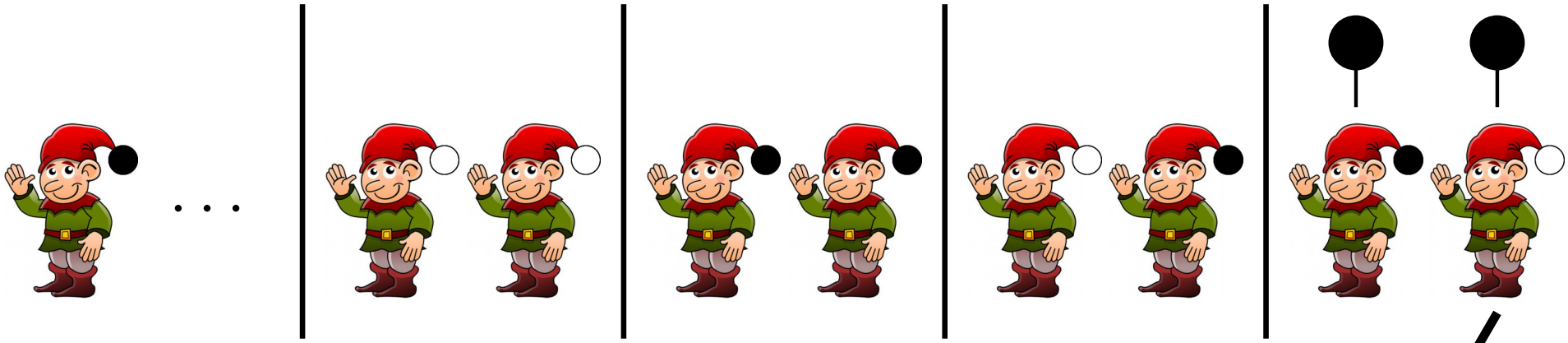
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

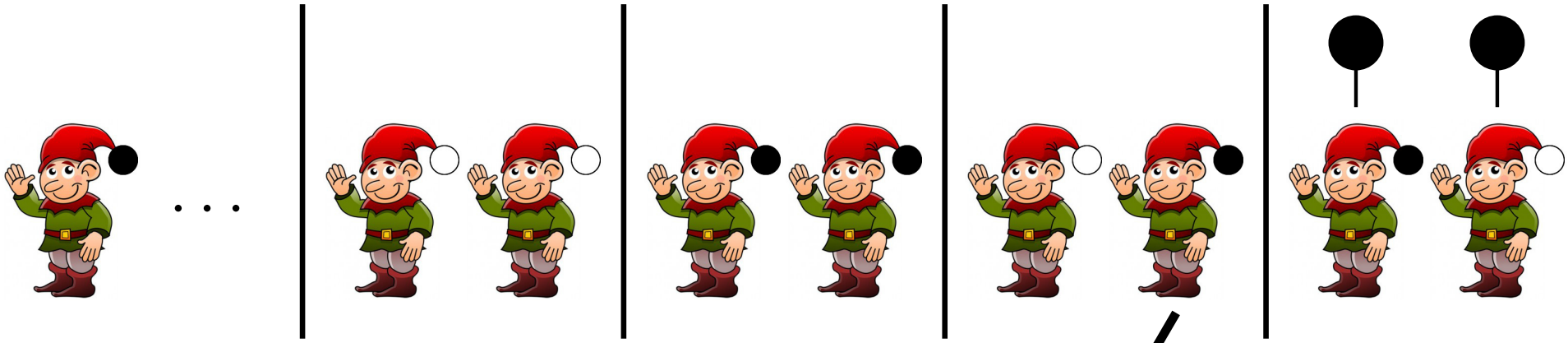
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

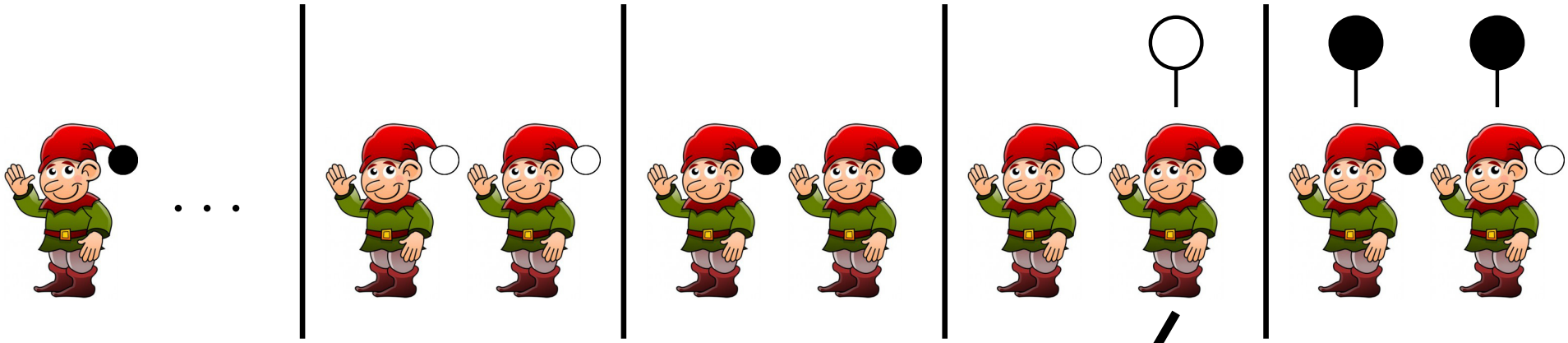
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

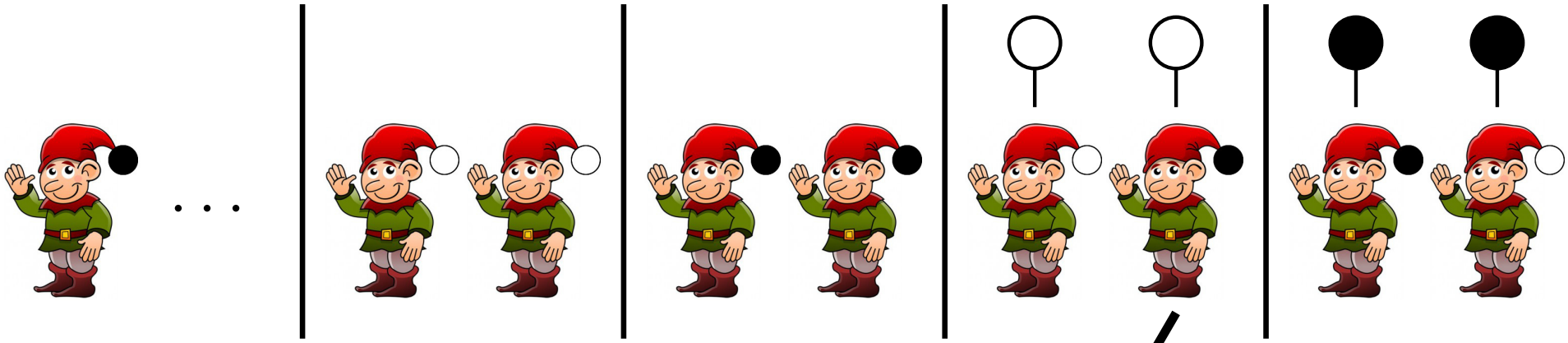
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

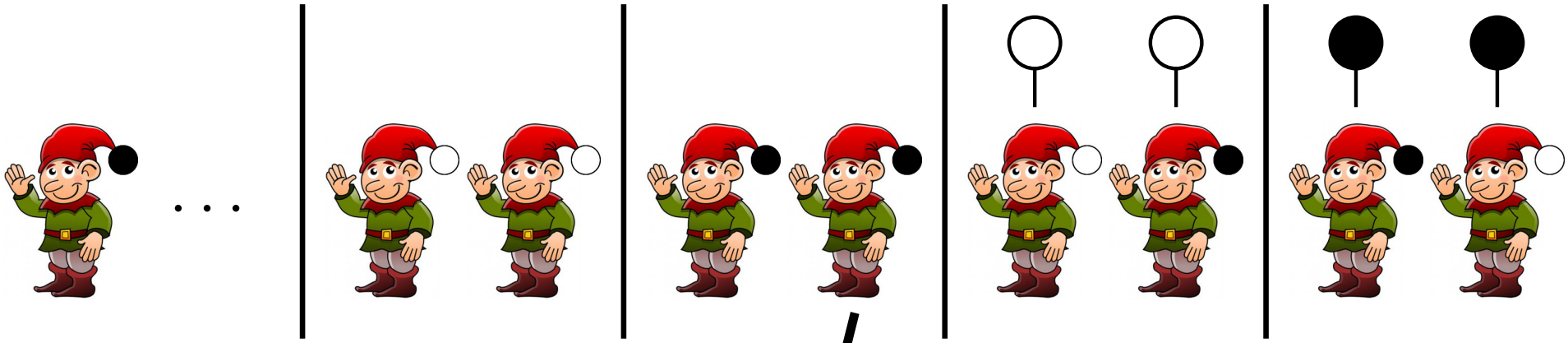
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

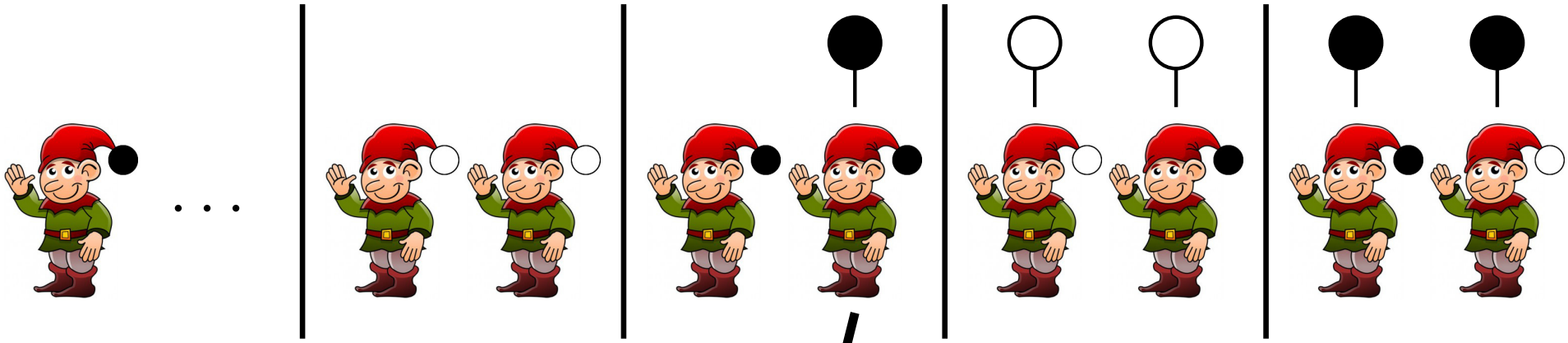
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

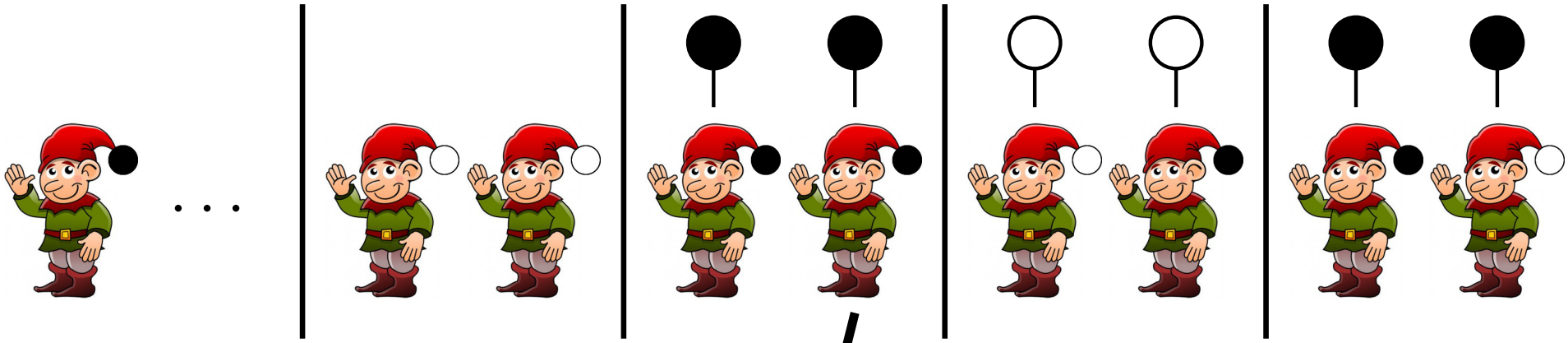
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

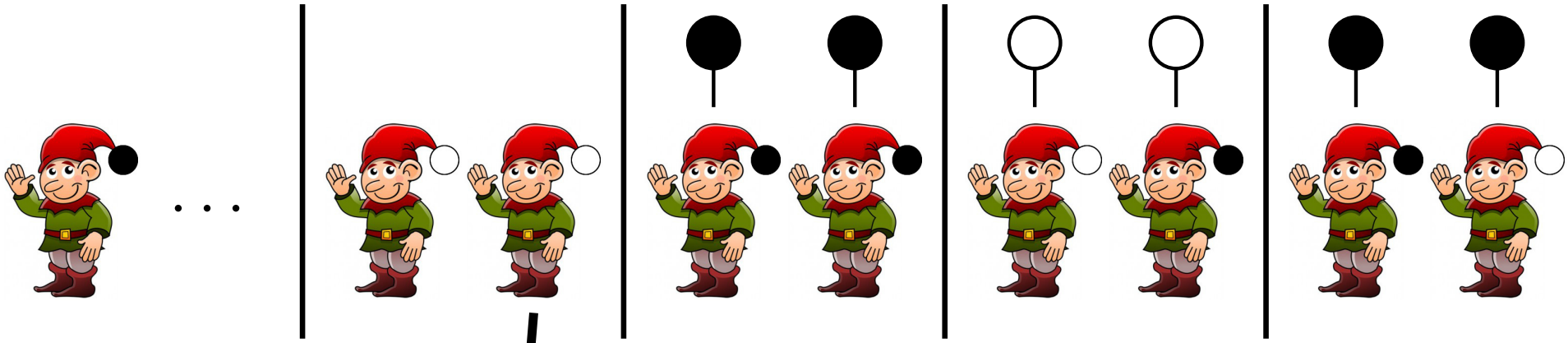
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

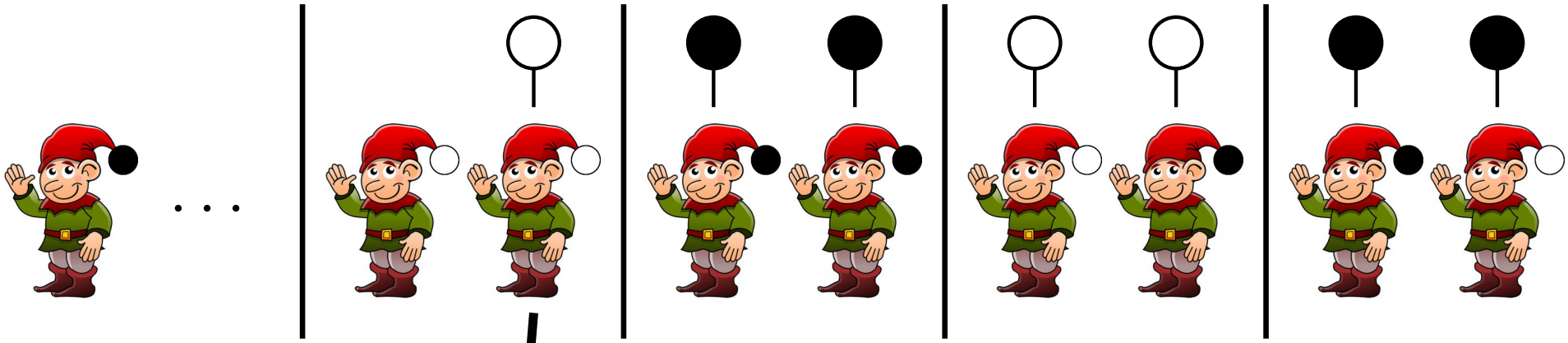
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

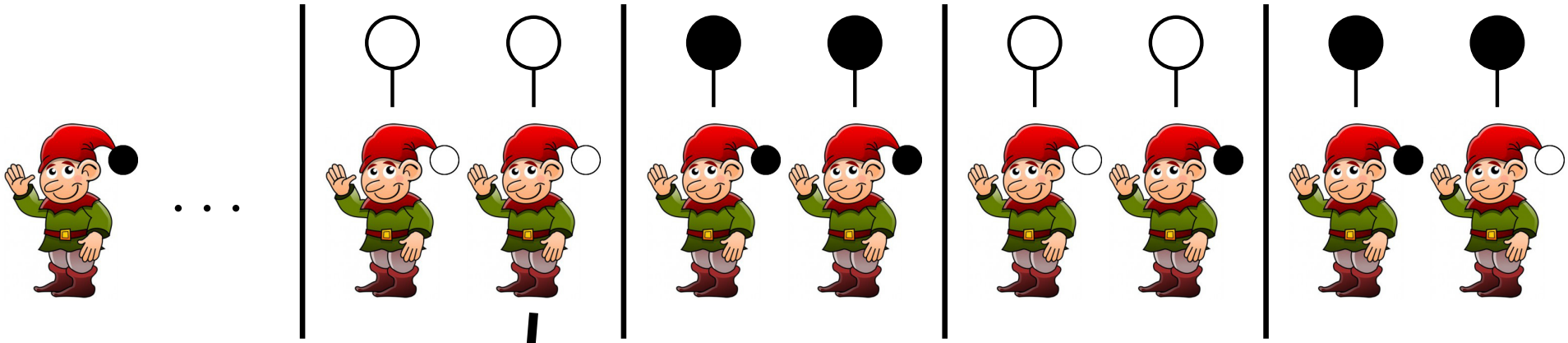
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

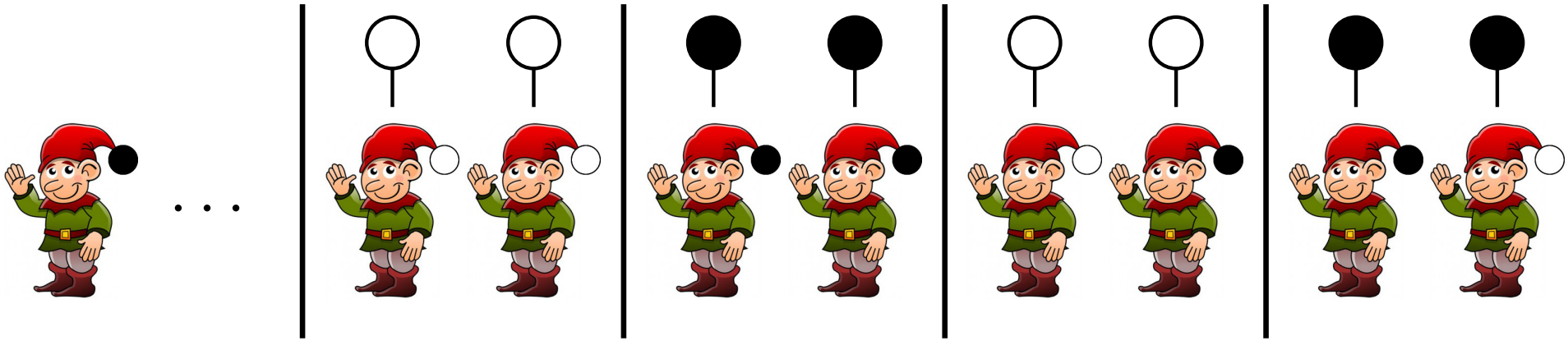
Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



Podpowiem mojemu poprzednikowi kolor jego pompona

Strategia I

Podzielmy krasnoludki na grupy dwukrasnoludkowe (od końca szeregu)



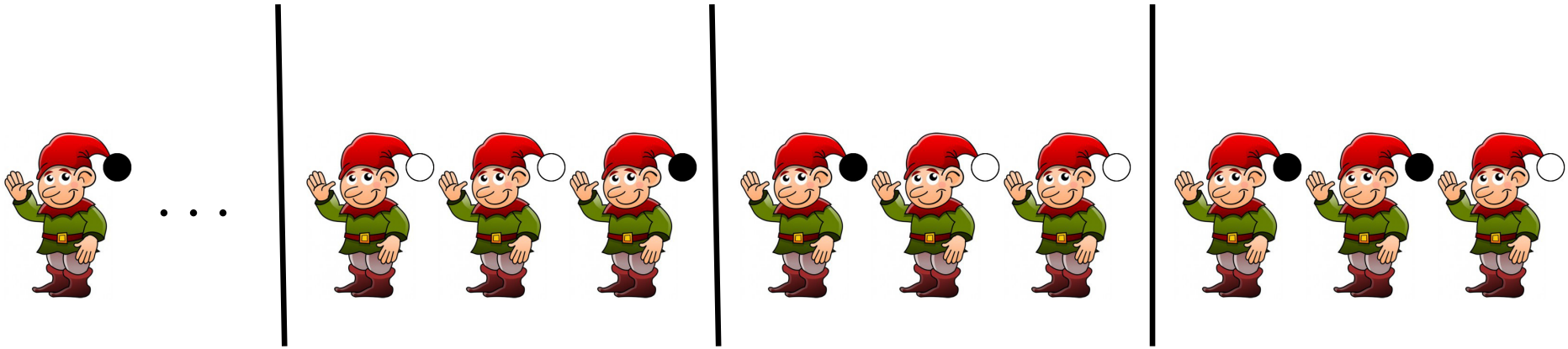
Podpowiem mojemu poprzednikowi kolor jego pompona

W ten sposób uratuje się co najmniej $\left\lfloor \frac{n}{2} \right\rfloor$ krasnoludków.
(W przypadku pesymistycznym uratuje się tylko $\left\lfloor \frac{n}{2} \right\rfloor$ krasnoludków.)

Strategia II

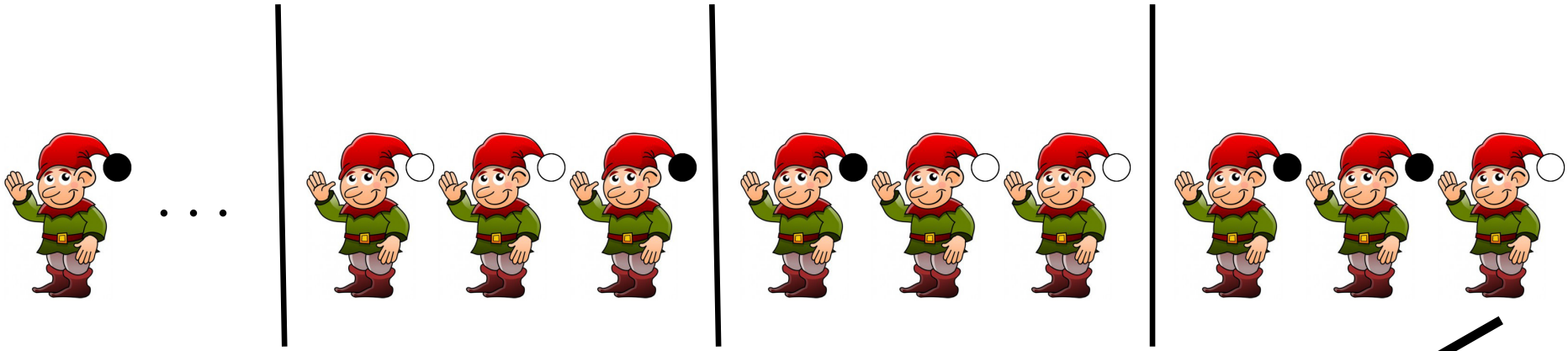
Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



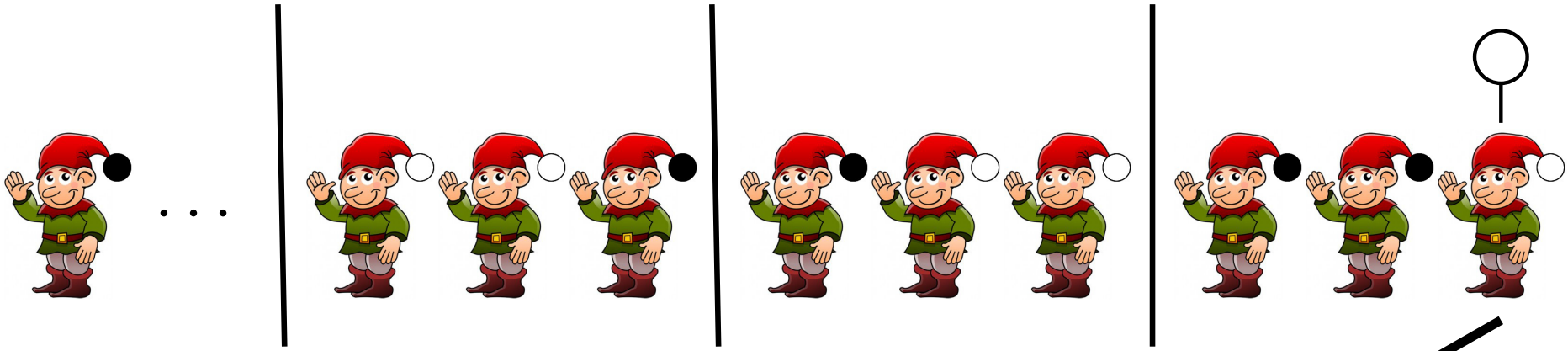
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



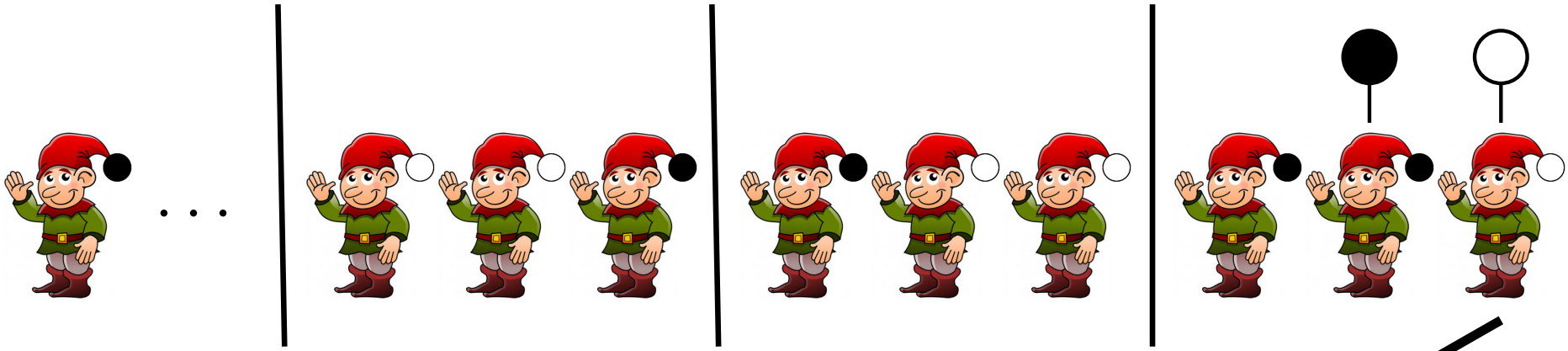
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



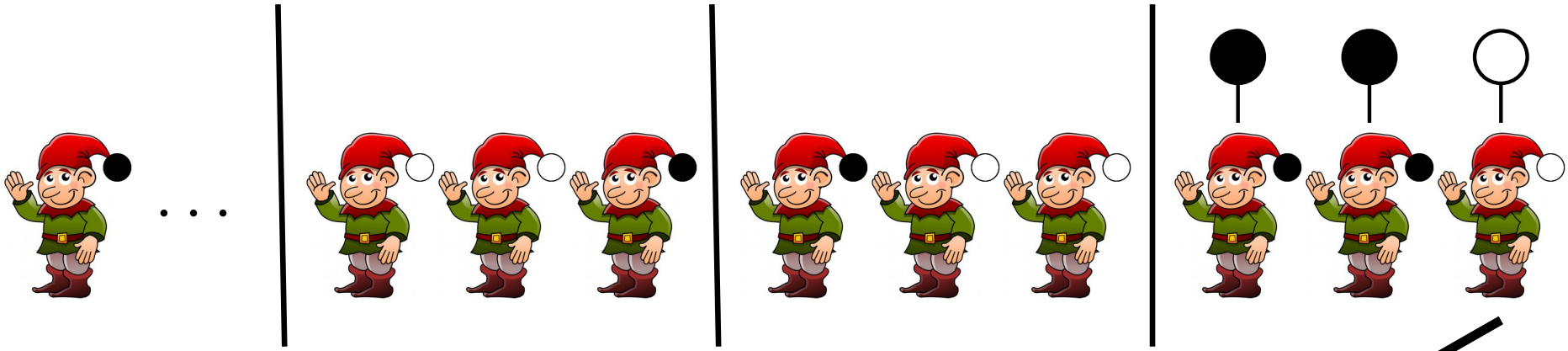
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



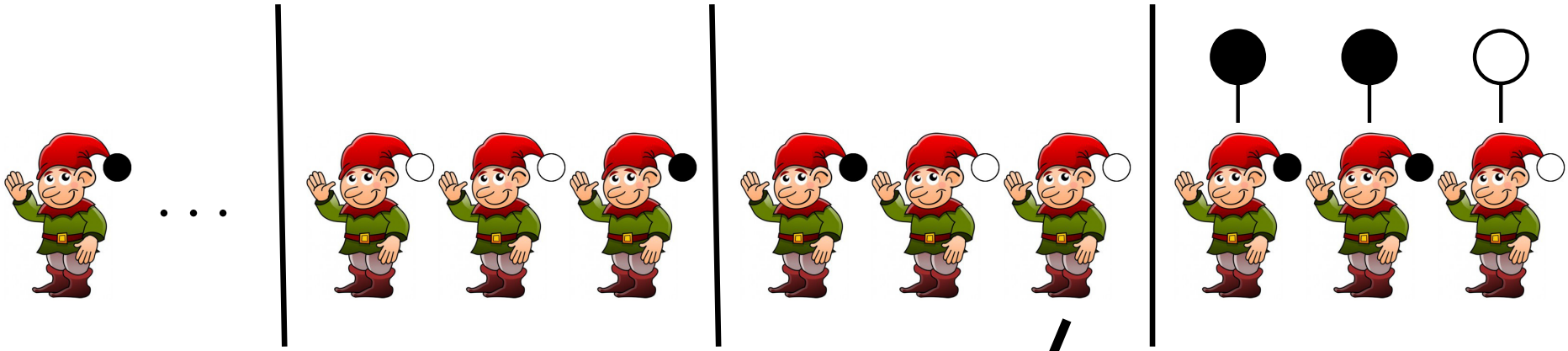
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



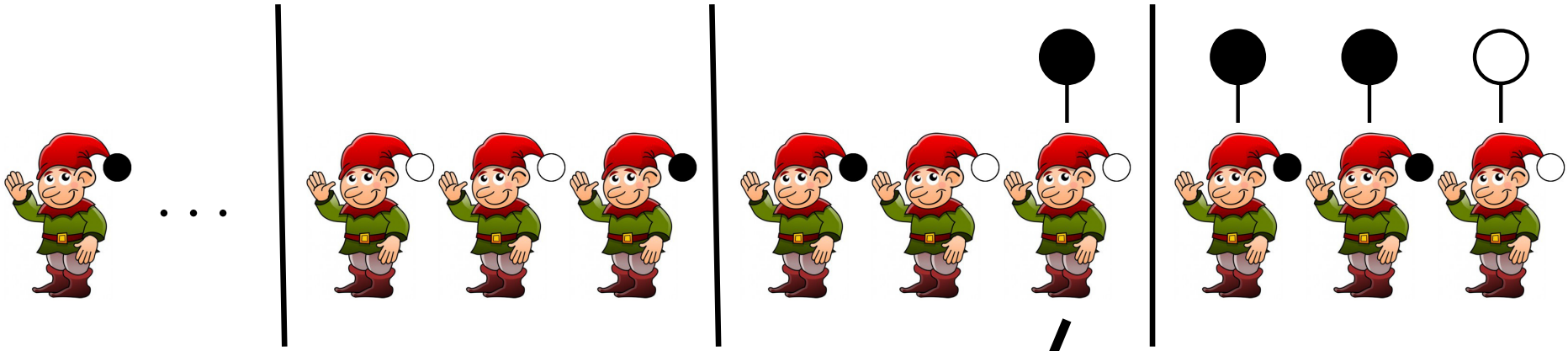
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



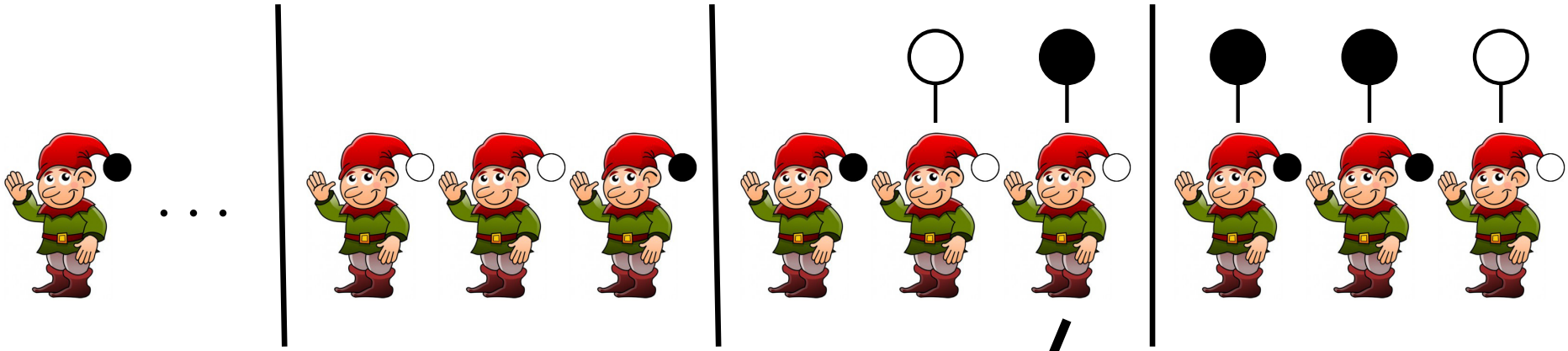
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



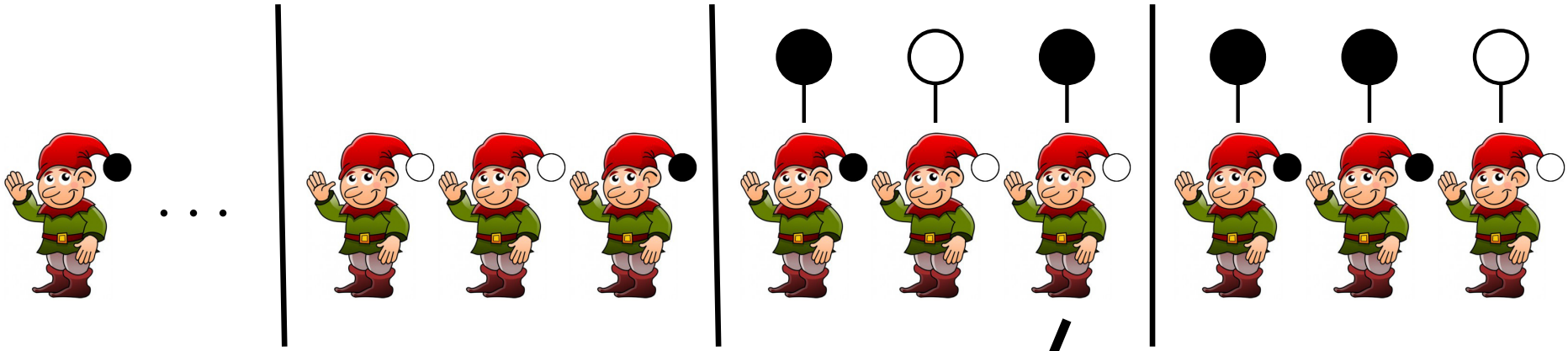
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



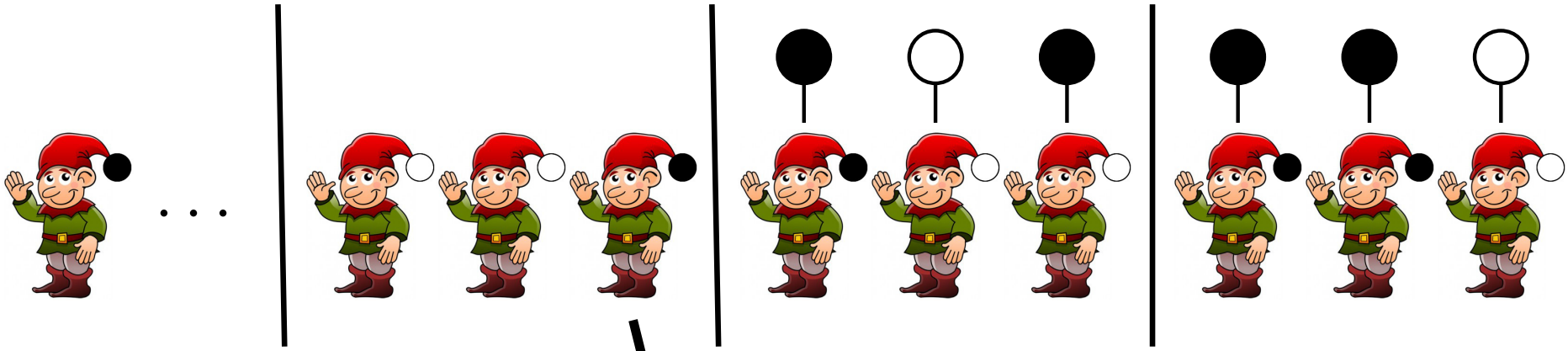
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



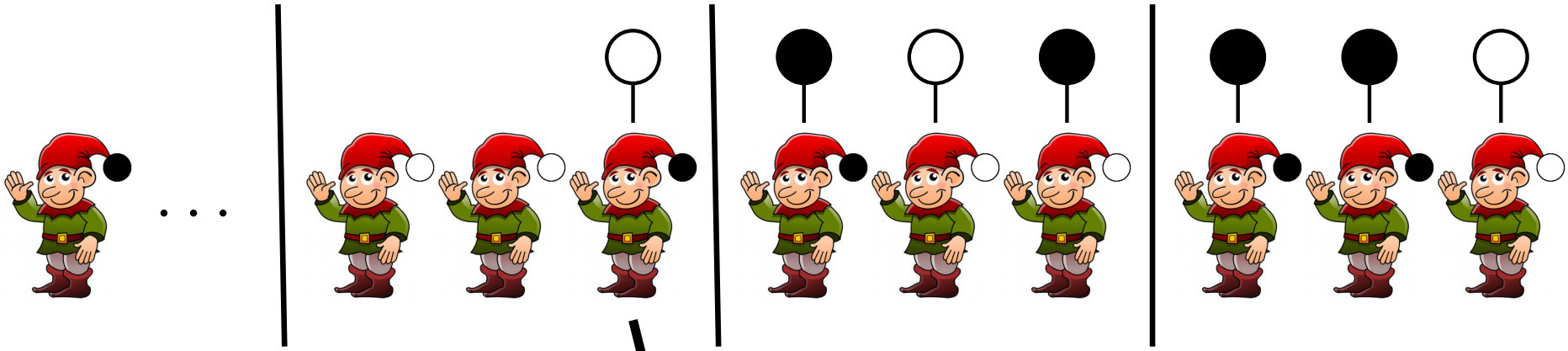
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



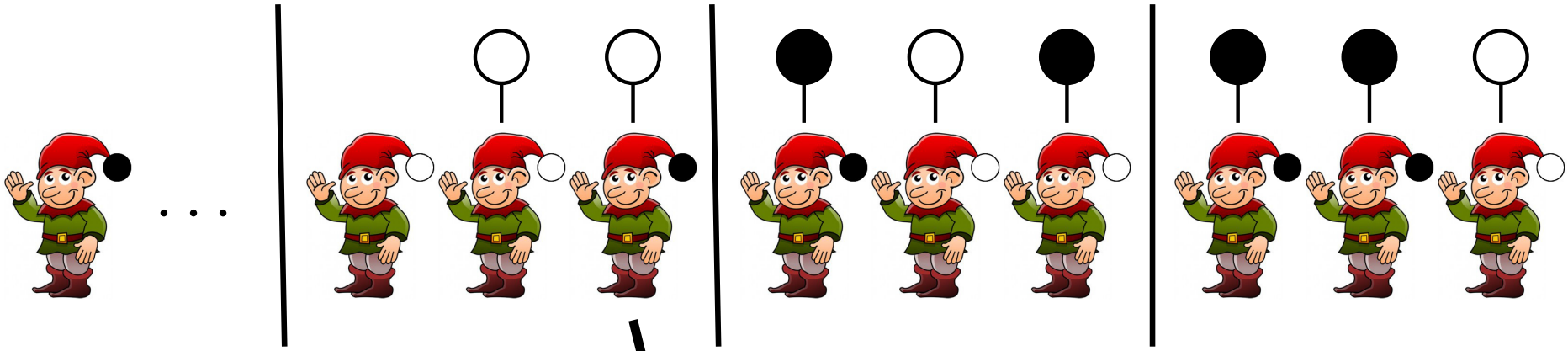
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



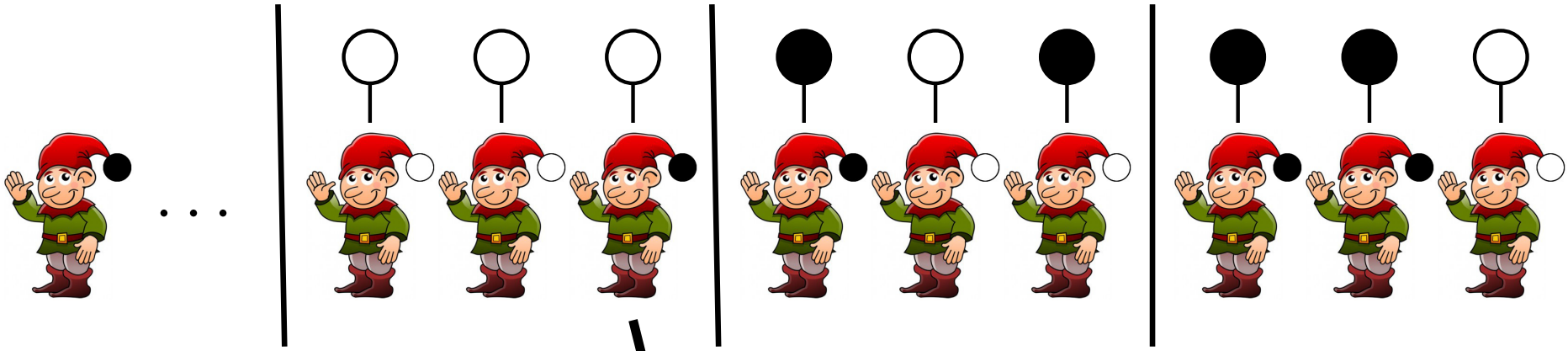
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



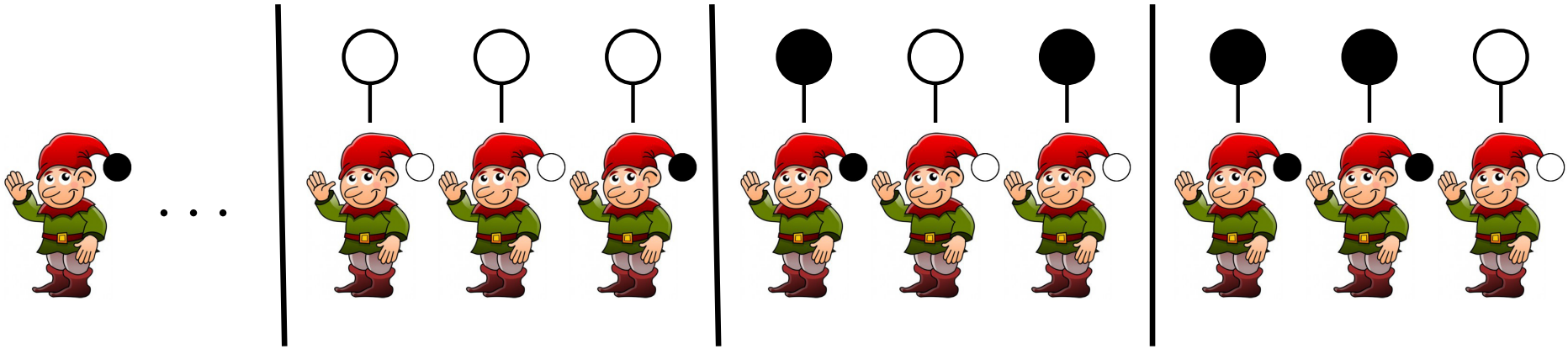
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

Strategia II

Podzielmy krasnoludki na grupy trójkrasnoludkowe (od końca szeregu)



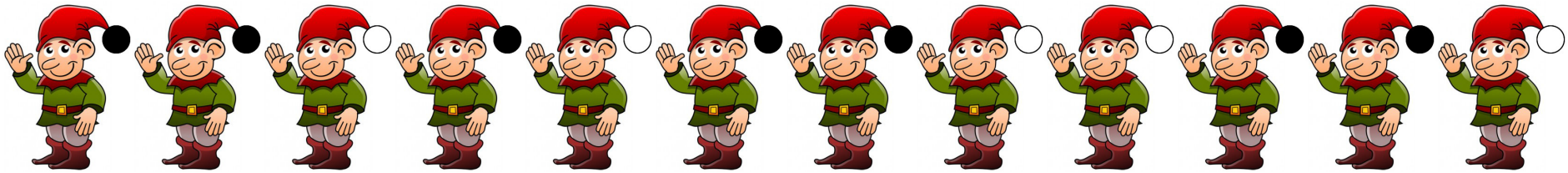
Podpowiem moim dwóm poprzednikom, czy mają pompony tego samego koloru:

○ – ten sam kolor

● – różne kolory

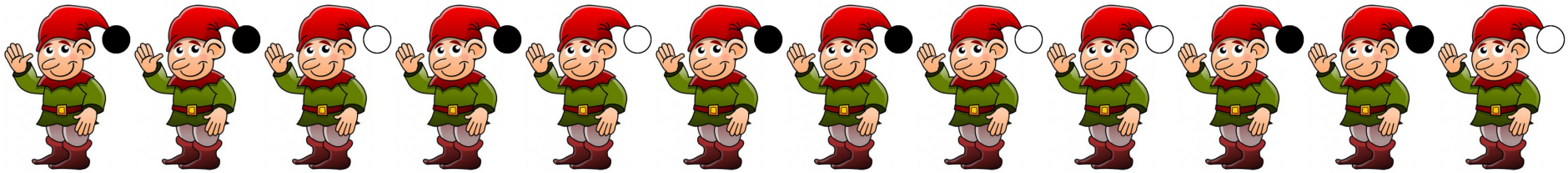
W ten sposób można uratować $\left\lfloor \frac{2}{3}n \right\rfloor$ krasnoludków.
(Lepiej, niż $\left\lfloor \frac{n}{2} \right\rfloor$.)

Strategia III



Strategia III

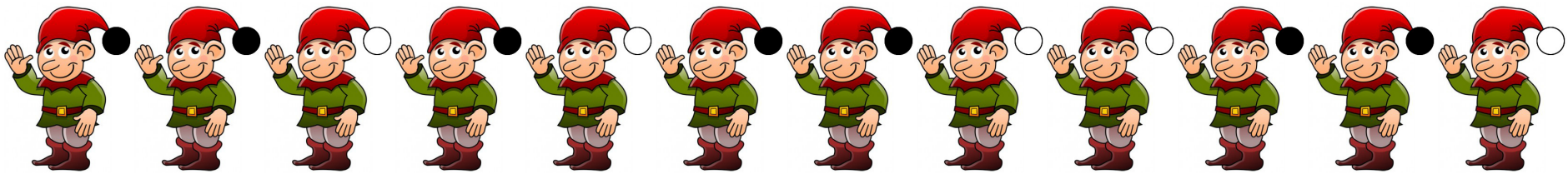
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



Strategia III

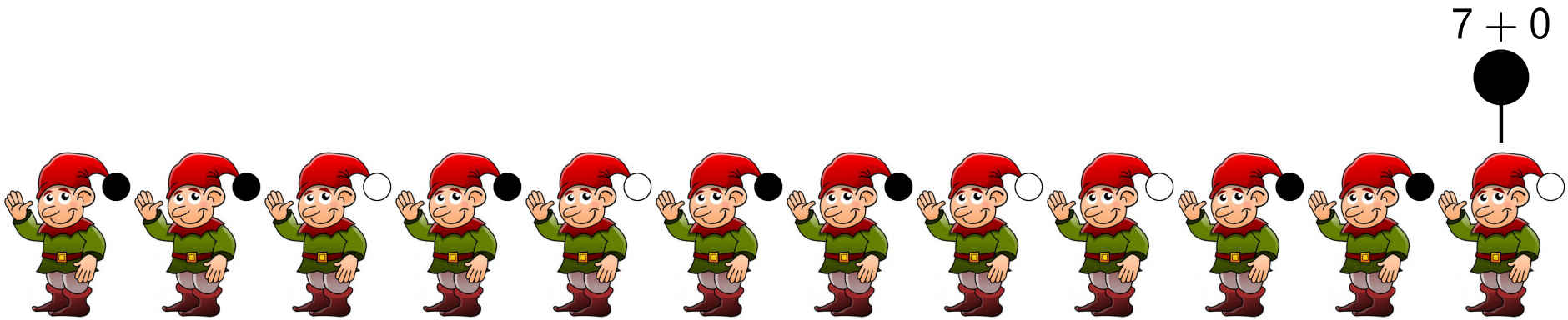
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta

$7 + 0$



Strategia III

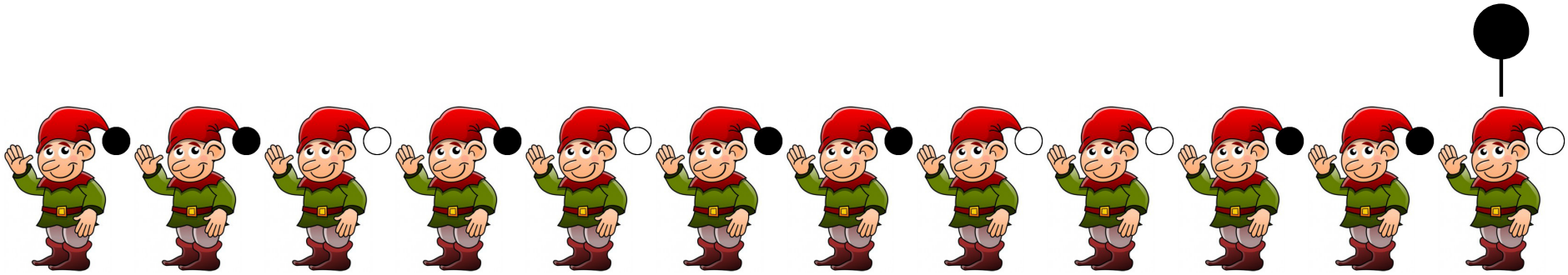
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



Strategia III

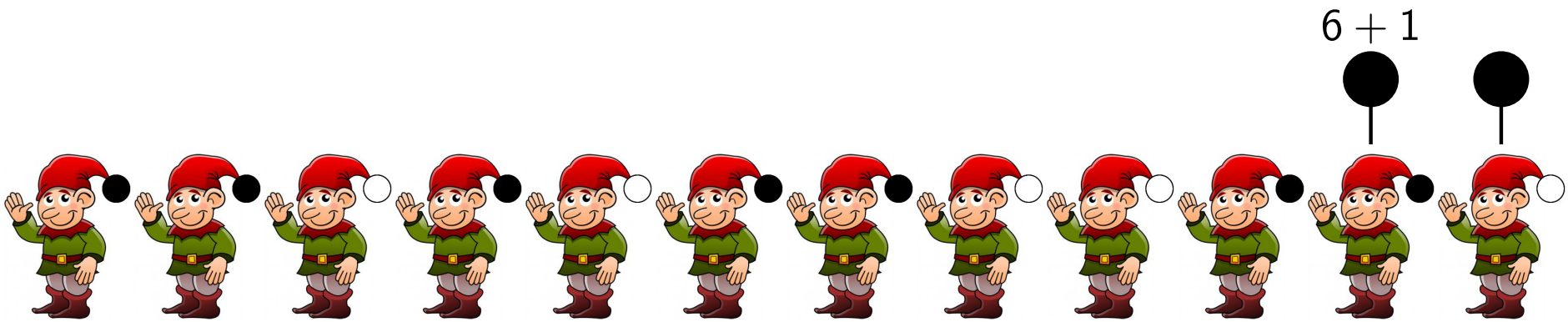
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta

$6 + 1$



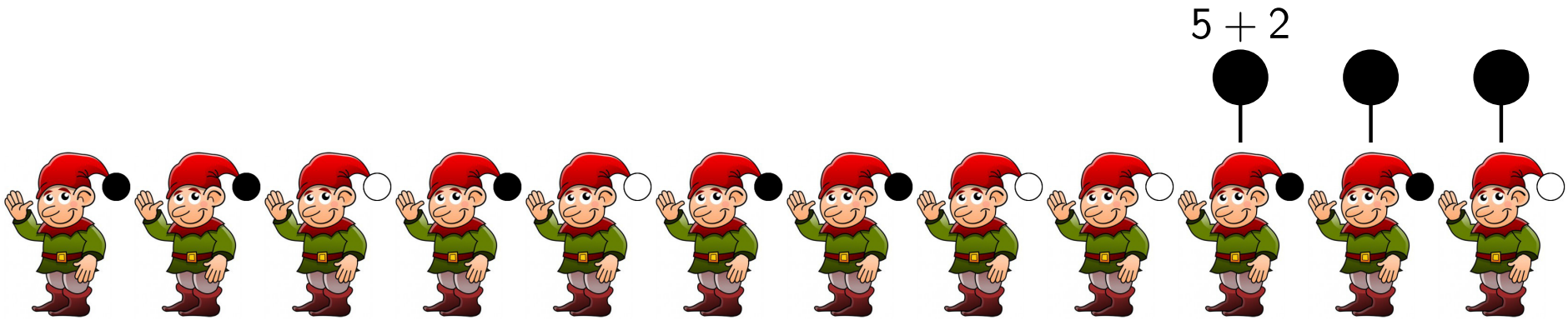
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



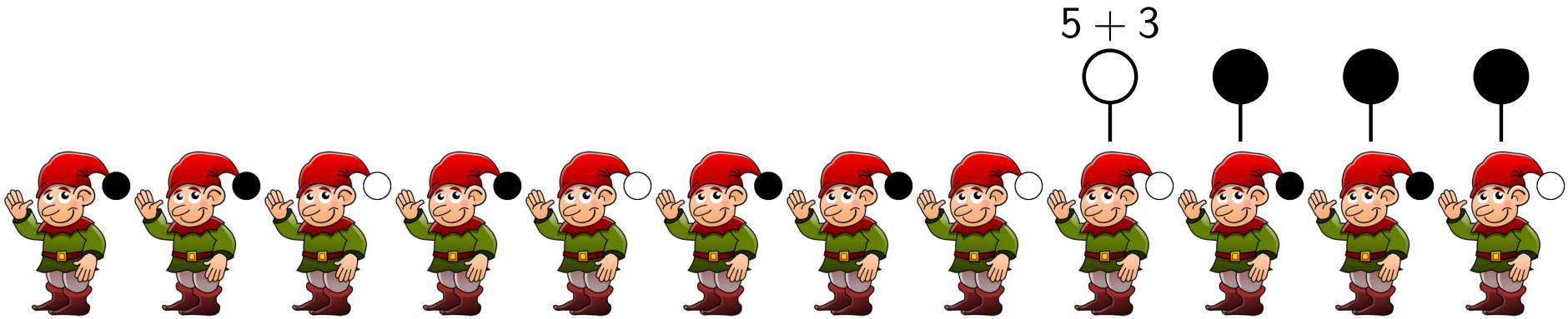
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



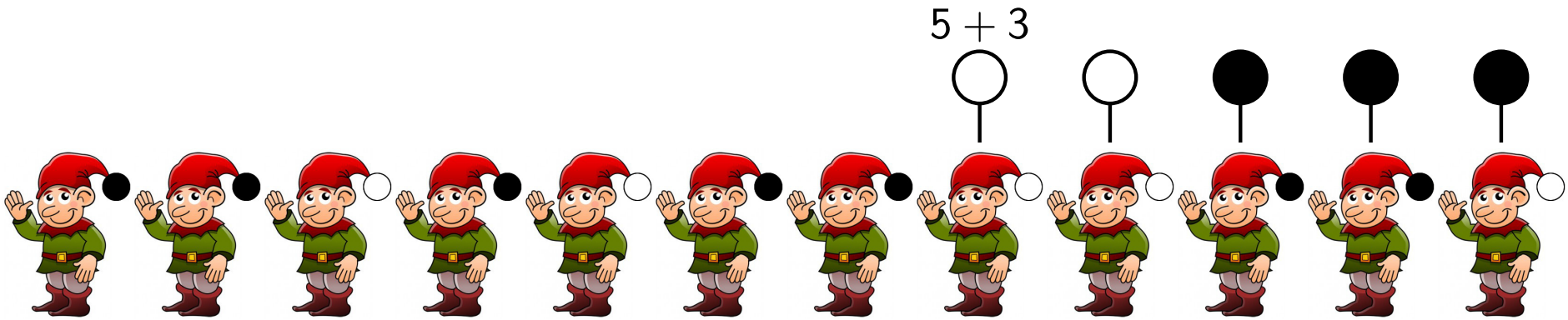
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



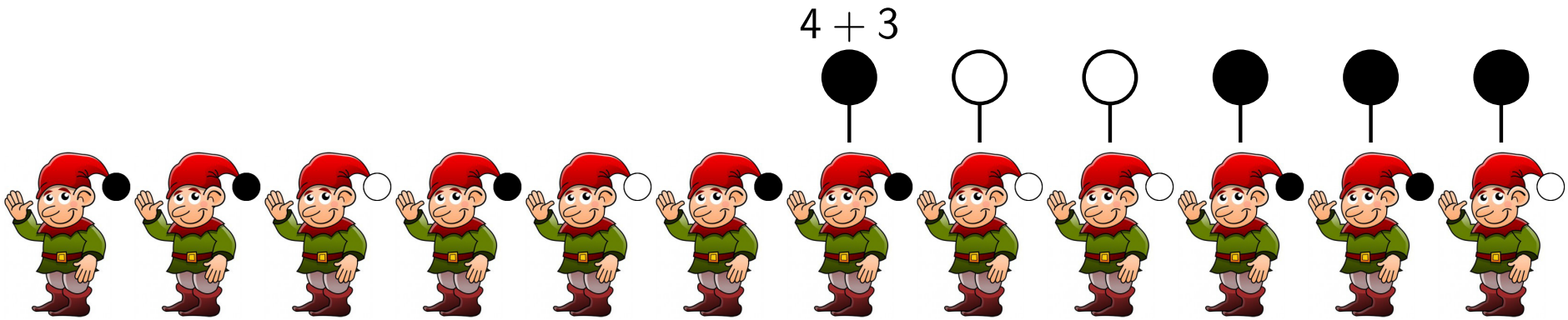
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



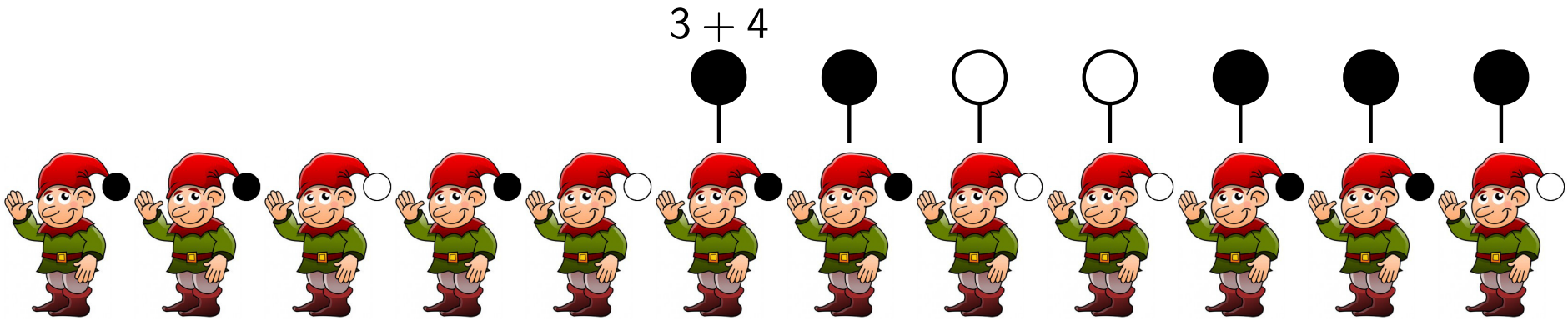
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



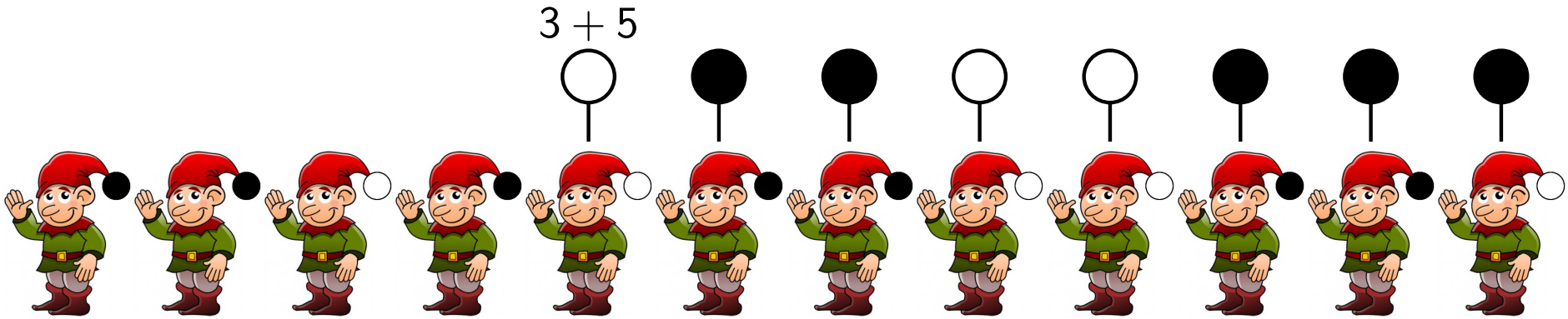
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



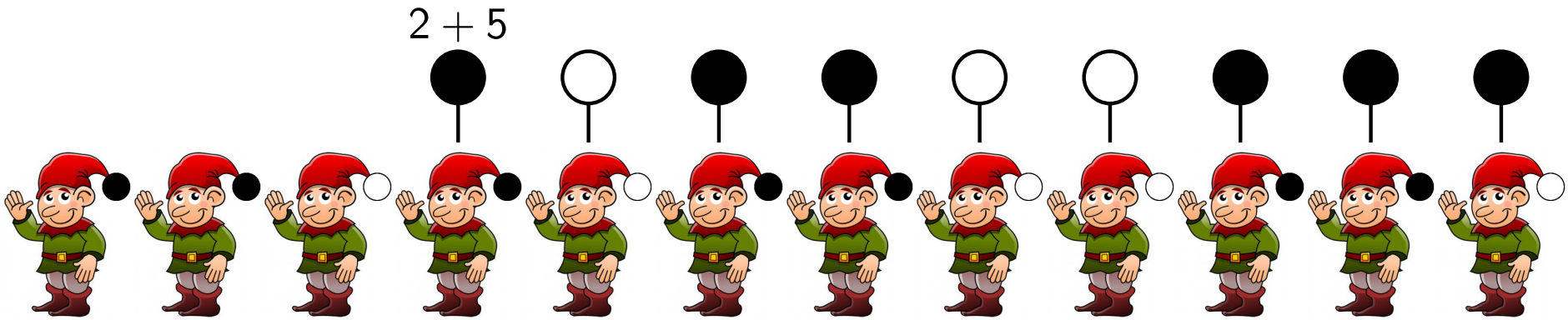
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



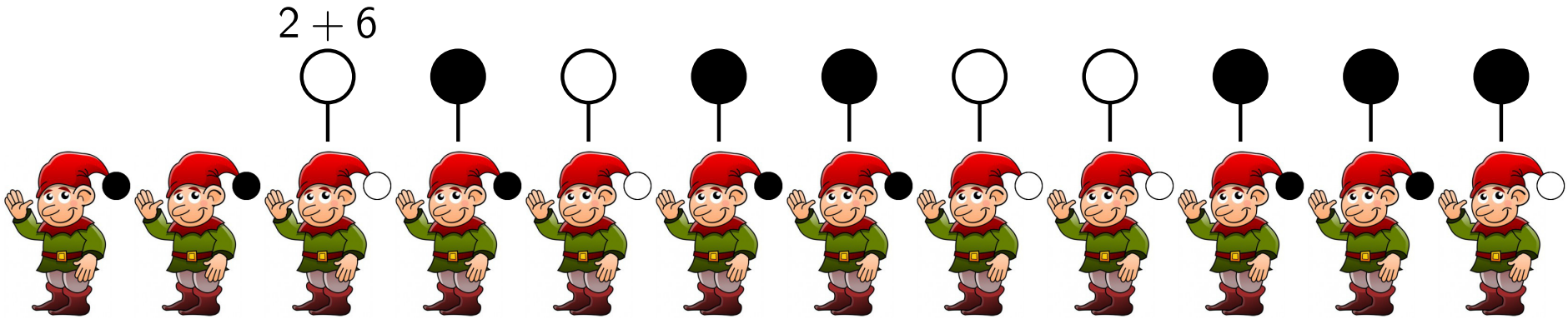
Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



Strategia III

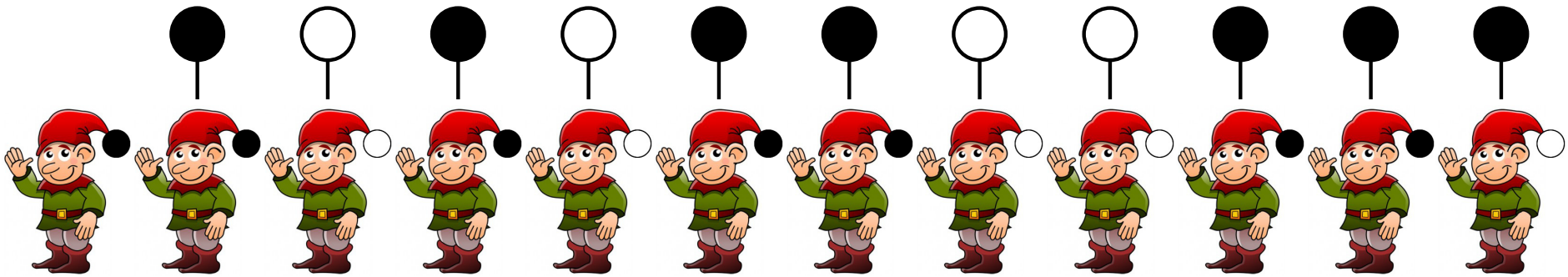
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta

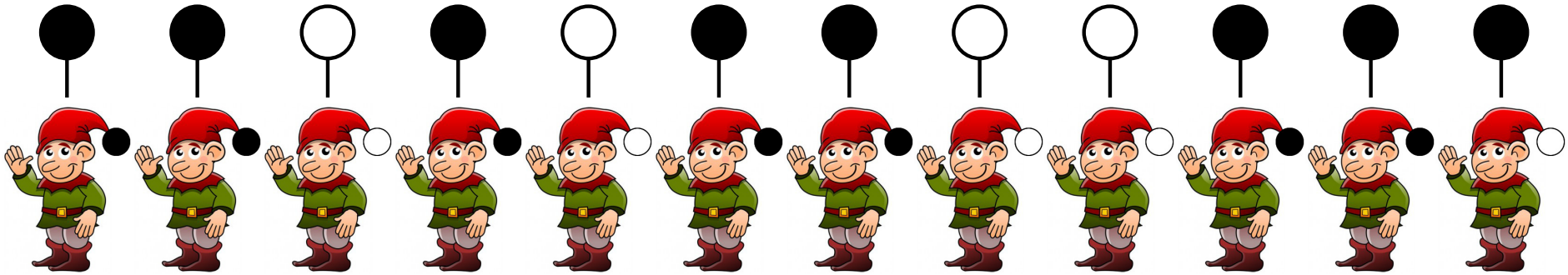
$1 + 6$



Strategia III

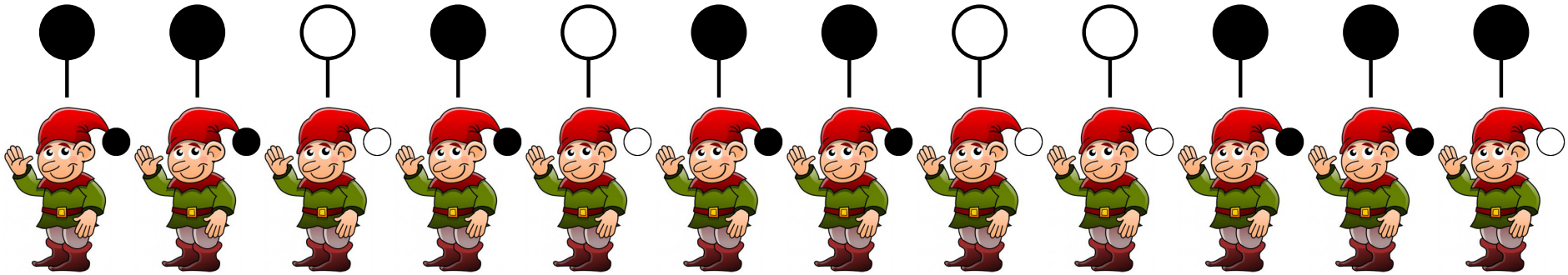
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta

$0 + 7$



Strategia III

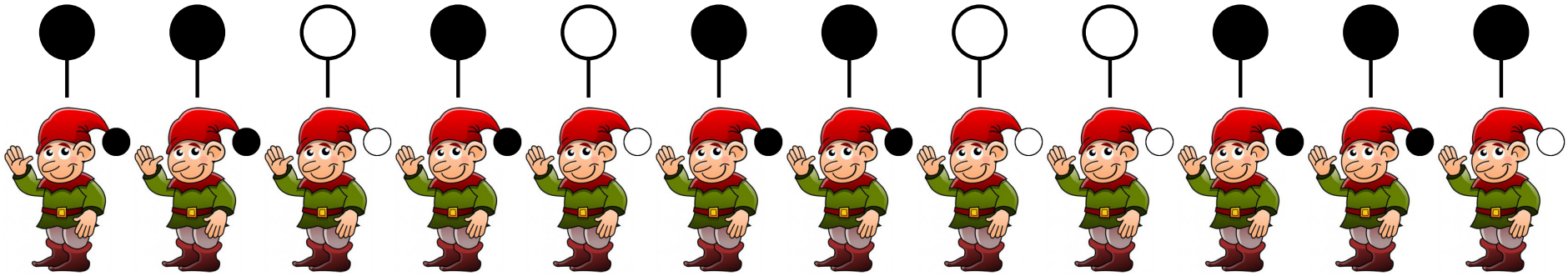
Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



W ten sposób można uratować aż $n - 1$ krasnoludków!
(Wszystkich oprócz ewentualnie tego na końcu szeregu.)

Strategia III

Krasnoludek mówi „czarny”, jeśli łączna liczba widzianych i „usłyszanych” czarnych pomponów jest nieparzysta



W ten sposób można uratować aż $n-1$ krasnoludków!
(Wszystkich oprócz ewentualnie tego na końcu szeregu.)

Niech ○ $= 0$ oraz ● $= 1$
a_i – kolor pompona krasnoludka i
b_i – kolor wypowiedziany przez krasnoludka i
Wówczas $$b_k = \bigoplus_{i<k} a_i \oplus \bigoplus_{j>k} b_j$$

A co to ma wspólnego z komputerami?
(Temat szkoły to *Matematyka i komputery*.)

A co to ma wspólnego z komputerami?
(Temat szkoły to *Matematyka i komputery*.)

Odp: BIT PARZYSTOŚCI

Jeśli wiemy, że w pewnym ciągu $x \in \{0,1\}^n$ jest parzysta liczba jedynek i jeśli któryś wyraz ciągu zaginie (i będziemy wiedzieć który) to będziemy w stanie go odzyskać (wyliczyć).
Tak zadziałały krasnoludki i ten sam mechanizm jest wykorzystywany w macierzach dyskowych RAID.

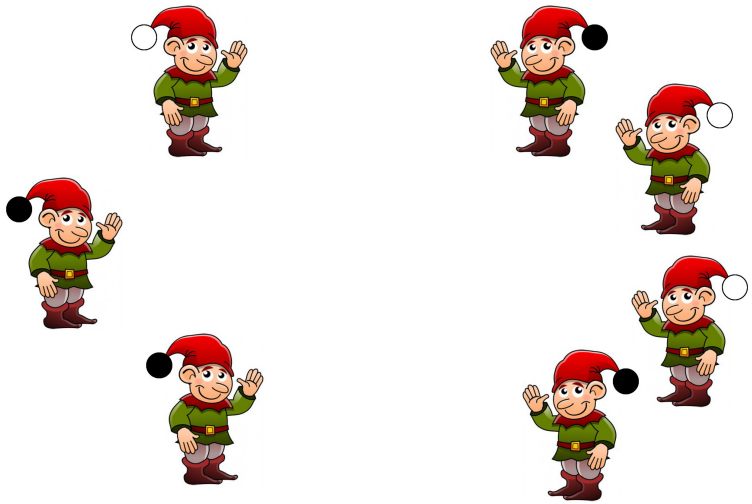
A co to ma wspólnego z komputerami?
(Temat szkoły to *Matematyka i komputery*.)

Odp: BIT PARZYSTOŚCI

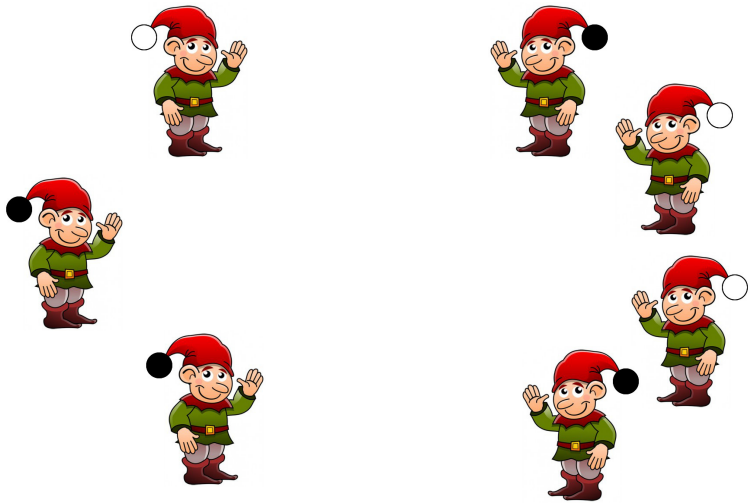
Jeśli wiemy, że w pewnym ciągu $x \in \{0,1\}^n$ jest parzysta liczba jedynek i jeśli któryś wyraz ciągu zaginie (i będziemy wiedzieć który) to będziemy w stanie go odzyskać (wyliczyć).
Tak zadziałały krasnoludki i ten sam mechanizm jest wykorzystywany w macierzach dyskowych RAID.

Jeśli z kolei będziemy przesyłać taki ciąg x i podczas przesyłania nieparzysta liczba wyrazów ciągu $x \in \{0,1\}^n$ ulegnie zaburzeniu ($0 \to 1$ lub $1 \to 0$) to co prawda nie będziemy w stanie stwierdzić, które wyrazy zostały zmienione, ale będziemy w stanie stwierdzić, że do zaburzenia doszło.

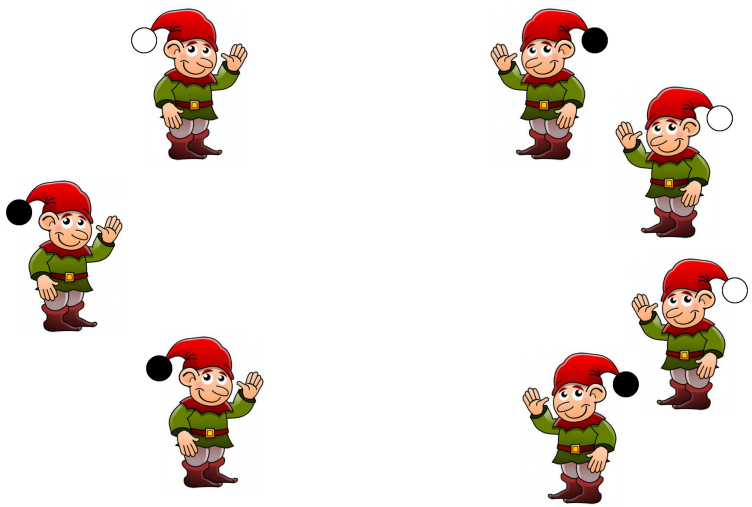
(Odległość Hamminga $d(x,y)$ dowolnych $x, y \in \{0,1\}^n$ mających parzystą liczbę jedynek jest parzysta.
$d(x,y) = |\{i : x_i \neq y_i\}|$ to liczba pozycji, na których x i y różnią się.)



Niezmiennie bardzo zła i cały czas brzydka czarownica zakłada krasnoludkom czapki z białymi lub czarnymi pomponami.



Niezmiennie bardzo zła i cały czas brzydka czarownica zakłada krasnoludkom czapki z białymi lub czarnymi pomponami.
Robi to losowo ($P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie). Każdy krasnoludek widzi kolory pomponów wszystkich czapek oprócz swojej.

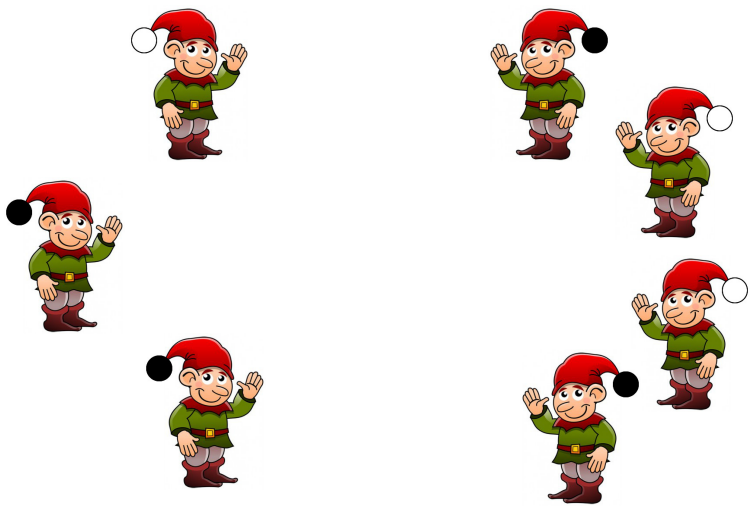


☐ Mam czarny pompon ●

☐ Mam biały pompon ○

☐ Nie wiem jaki mam pompon

Niezmiennie bardzo zła i cały czas brzydka czarownica zakłada krasnoludkom czapki z białymi lub czarnymi pomponami.
Robi to losowo ($P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie). Każdy krasnoludek widzi kolory pomponów wszystkich czapek oprócz swojej.
Każdy krasnoludek ma odgadnąć kolor swojego pompona wypełniając ankietę.



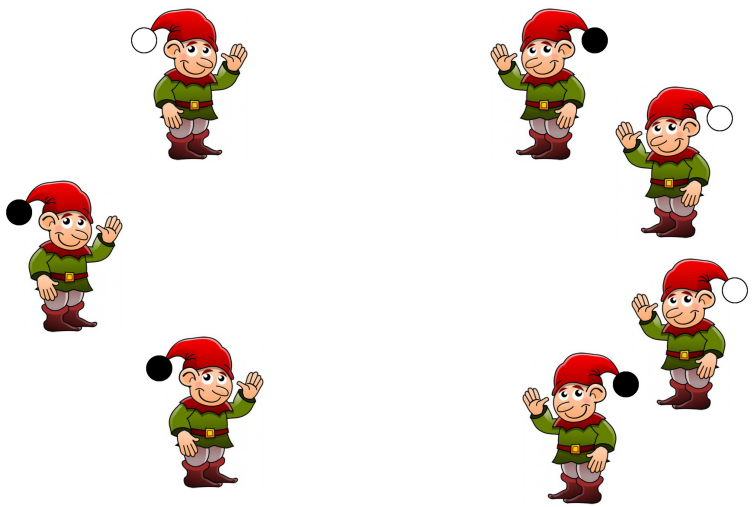
☐ Mam czarny pompon ●

☐ Mam biały pompon ○

☐ Nie wiem jaki mam pompon

Niezmiennie bardzo zła i cały czas brzydka czarownica zakłada krasnoludkom czapki z białymi lub czarnymi pomponami.
Robi to losowo ($P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie). Każdy krasnoludek widzi kolory pomponów wszystkich czapek oprócz swojej.
Każdy krasnoludek ma odgadnąć kolor swojego pompona wypełniając ankietę.

Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną ugotowane i zjedzone przez czarownicę.



☐ Mam czarny pompon ●

☐ Mam biały pompon ○

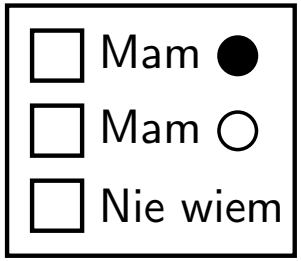
☐ Nie wiem jaki mam pompon

Niezmiennie bardzo zła i cały czas brzydka czarownica zakłada krasnoludkom czapki z białymi lub czarnymi pomponami.
Robi to losowo ($P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie). Każdy krasnoludek widzi kolory pomponów wszystkich czapek oprócz swojej.
Każdy krasnoludek ma odgadnąć kolor swojego pompona wypełniając ankietę.

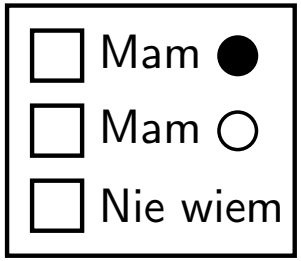
Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną ugotowane i zjedzone przez czarownicę.

Pomóżmy krasnoludkom! Wymyślmy taką strategię, by z możliwie dużym prawdopodobieństwem uratowały się.

n krasnoludków z losowymi pomponami
$P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie
Każdy widzi wszystkie pompony oprócz swojego



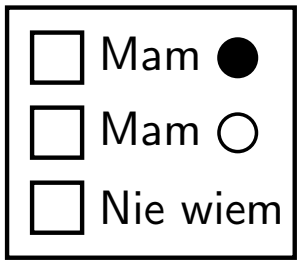
Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną zjedzone.
Chcemy zmaksymalizować prawdopodobieństwo niezjedzenia.



n krasnoludków z losowymi pomponami
$P(○) = P(●) = \frac{1}{2}$; niezależnie
Każdy widzi wszystkie pompony oprócz swojego
Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną zjedzone.
Chcemy zmaksymalizować prawdopodobieństwo niezjedzenia.

Zdrowy rozsądek podpowiada, że nie da się uzyskać prawdopodobieństwa niezjedzenia większego niż $\frac{1}{2}$.

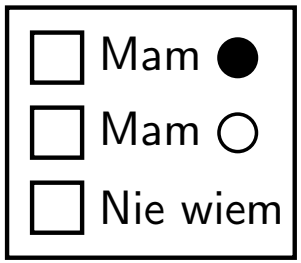
n krasnoludków z losowymi pomponami
$P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie
Każdy widzi wszystkie pompony oprócz swojego



Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną zjedzone.
Chcemy zmaksymalizować prawdopodobieństwo niezjedzenia.

Zdrowy rozsądek podpowiada, że nie da się uzyskać prawdopodobieństwa niezjedzenia większego niż $\frac{1}{2}$.

Okazuje się jednak, że można uzyskać więcej niż $\frac{1}{2}$: Pokażę, że gdy liczba krasnoludków jest postaci $n = 2^k - 1$, to mądre krasnoludki uratują się z prawdopodobieństwem $\frac{n}{n+1} = 1 - \frac{1}{2^k}$.



n krasnoludków z losowymi pomponami
$P(\bigcirc) = P(\bullet) = \frac{1}{2}$; niezależnie
Każdy widzi wszystkie pompony oprócz swojego
Jeśli choć jeden krasnoludek poda błędny kolor lub wszystkie odpowiedzą „Nie wiem” to wszystkie zostaną zjedzone.
Chcemy zmaksymalizować prawdopodobieństwo niezjedzenia.

Strategia (dla $n = 2^k - 1$; dająca $P(\text{niezjedzenie}) = \frac{n}{n+1} = 1 - \frac{1}{2^k}$)

Numerujemy krasnoludki (a właściwie pompony) liczbami od 1 do $n = 2^k - 1$. Każdy krasnoludek widząc inne pompony odpowiada:

Mam ●	gdy XOR numerów czarnych pomponów to 0
Mam ○	gdy XOR numerów czarnych pomponów to mój numer
Nie wiem	w pozostałych przypadkach

Strategia (dla $n = 2^k - 1$; dająca $P(\text{niezjedzenie}) = \frac{n}{n+1} = 1 - \frac{1}{2^k}$)

Numery pomponów: $1, 2, \ldots, n$. Każdy krasnoludek odpowiada:

Mam ●	gdy XOR numerów czarnych pomponów to 0
Mam ○	gdy XOR numerów czarnych pomponów to mój numer
Nie wiem	w pozostałych przypadkach

Dlaczego to działa?

Strategia (dla $n = 2^k - 1$; dająca $P(\text{niezjedzenie}) = \frac{n}{n+1} = 1 - \frac{1}{2^k}$)

Numery pomponów: $1, 2, \ldots, n$. Każdy krasnoludek odpowiada:

Mam ●	gdy XOR numerów czarnych pomponów to 0
Mam ○	gdy XOR numerów czarnych pomponów to mój numer
Nie wiem	w pozostałych przypadkach

Niech $w =$ XOR numerów wszystkich czarnych pomponów.
Przypadek I: $w \neq 0$. Rozważmy krasnoludka i.

Jeśli $i \neq w$, to niezależnie od koloru własnego pompona krasnoludek i odpowie „Nie wiem" (bo $w, w \oplus i \notin \{0, i\}$)

Jeśli $i = w$ i krasnoludek i ma biały pompon, to odpowie on „Mam ○" (bo $w = i$)

Jeśli $i = w$ i krasnoludek i ma czarny pompon, to odpowie on „Mam ●" (bo $w \oplus i = 0$)

Krasnoludki są uratowane! ☺

Strategia (dla $n = 2^k - 1$; dająca $P(\text{niezjedzenie}) = \frac{n}{n+1} = 1 - \frac{1}{2^k}$)

Numery pomponów: $1, 2, \ldots, n$. Każdy krasnoludek odpowiada:

Mam ●	gdy XOR numerów czarnych pomponów to 0
Mam ○	gdy XOR numerów czarnych pomponów to mój numer
Nie wiem	w pozostałych przypadkach

Niech $w =$ XOR numerów wszystkich czarnych pomponów.
Przypadek II: $w = 0$. Rozważmy krasnoludka i.

Jeśli krasnoludek i ma biały pompon, to odpowie on „Mam ●" (bo $w = 0$)

Jeśli krasnoludek i ma czarny pompon, to odpowie on „Mam ○" (bo $w \oplus i = 0 \oplus i = i$)

Krasnoludki zostaną zjedzone! ☹

Strategia (dla $n = 2^k - 1$; dająca $P(\text{niezjedzenie}) = \frac{n}{n+1} = 1 - \frac{1}{2^k}$)

Numery pomponów: $1, 2, \ldots, n$. Każdy krasnoludek odpowiada:

Mam ●	gdy XOR numerów czarnych pomponów to 0
Mam ○	gdy XOR numerów czarnych pomponów to mój numer
Nie wiem	w pozostałych przypadkach

Niech $w =$ XOR numerów wszystkich czarnych pomponów.

Podsumowując:

Krasnoludki uratują się wtedy i tylko wtedy, gdy $w \neq 0$.

Prawdopodobieństwo, że $w \neq 0$ wynosi $1 - \frac{1}{2^k} = \frac{n}{n+1}$

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0, 1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0,1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

Własności zbioru $\mathcal{C}$

- $\mathcal{C} \subset \{0,1\}^n = \{0,1\}^{2^k-1}$,
- $|\mathcal{C}| = \frac{2^n}{2^k} = 2^{n-k} = 2^{2^k-k-1}$,

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0,1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

Własności zbioru $\mathcal{C}$

- $\mathcal{C} \subset \{0,1\}^n = \{0,1\}^{2^k-1}$,
- $|\mathcal{C}| = \frac{2^n}{2^k} = 2^{n-k} = 2^{2^k-k-1}$,
- Jeśli $x, y \in \mathcal{C}$ i $x \neq y$, to $d(x,y) \geqslant 3$ (bo $\bigoplus_{i:x_i \neq y_i} i = 0$),

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0,1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

Własności zbioru $\mathcal{C}$

- $\mathcal{C} \subset \{0,1\}^n = \{0,1\}^{2^k-1}$,
- $|\mathcal{C}| = \frac{2^n}{2^k} = 2^{n-k} = 2^{2^k-k-1}$,
- Jeśli $x, y \in \mathcal{C}$ i $x \neq y$, to $d(x,y) \geqslant 3$ (bo $\bigoplus_{i:x_i \neq y_i} i = 0$),
- $\forall_{z \in \{0,1\}^n} \exists_{x \in \mathcal{C}} d(x,z) \leqslant 1$ (aby dostać $x \in \mathcal{C}$ wystarczy zmienić z na pozycji $\bigoplus_{i:z_i=1} i$).

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0,1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

Własności zbioru $\mathcal{C}$

- $\mathcal{C} \subset \{0,1\}^n = \{0,1\}^{2^k-1}$,
- $|\mathcal{C}| = \frac{2^n}{2^k} = 2^{n-k} = 2^{2^k-k-1}$,
- Jeśli $x, y \in \mathcal{C}$ i $x \neq y$, to $d(x,y) \geqslant 3$ (bo $\bigoplus_{i:x_i \neq y_i} i = 0$),
- $\forall_{z \in \{0,1\}^n} \exists_{x \in \mathcal{C}} d(x,z) \leqslant 1$ (aby dostać $x \in \mathcal{C}$ wystarczy zmienić z na pozycji $\bigoplus_{i:z_i=1} i$).

Geometrycznie: Kule o promieniach 1 i o środkach w elementach $\mathcal{C}$ są parami rozłączne i wypełniają $\{0,1\}^n$.

A co to ma wspólnego z komputerami? (*Matematyka i komputery*)

Odp: Kod Hamminga $[2^k - 1, 2^k - k - 1, 3]_2$

Niech $n = 2^k - 1$ i rozważmy zbiór $\mathcal{C} \subset \{0,1\}$ złożony z tych układów kolorów pomponów, dla których krasnoludki zostaną zjedzone.

$x \in \mathcal{C} \Leftrightarrow \bigoplus_{i:x_i=1} i = 0.$

Własności zbioru $\mathcal{C}$

- $\mathcal{C} \subset \{0,1\}^n = \{0,1\}^{2^k-1}$,
- $|\mathcal{C}| = \frac{2^n}{2^k} = 2^{n-k} = 2^{2^k-k-1}$,
- Jeśli $x, y \in \mathcal{C}$ i $x \neq y$, to $d(x,y) \geqslant 3$ (bo $\bigoplus_{i:x_i \neq y_i} i = 0$),
- $\forall_{z \in \{0,1\}^n} \exists_{x \in \mathcal{C}} d(x,z) \leqslant 1$ (aby dostać $x \in \mathcal{C}$ wystarczy zmienić z na pozycji $\bigoplus_{i:z_i=1} i$).

Geometrycznie: Kule o promieniach 1 i o środkach w elementach $\mathcal{C}$ są parami rozłączne i wypełniają $\{0,1\}^n$.

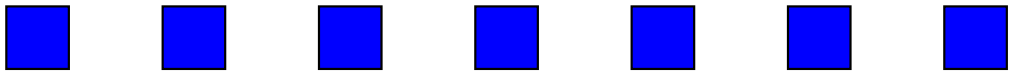
Efekt: Jeśli będziemy przesyłać ciąg $x \in \mathcal{C}$ i podczas przesyłania ulegnie on zaburzeniu ($0 \to 1$ lub $1 \to 0$) na jednej pozycji, to nie tylko wykryjemy ten błąd, ale także go naprawimy.

Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?

Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).

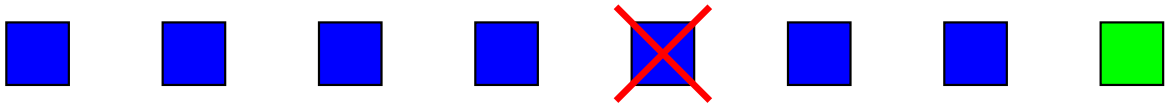
Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?

Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$)

Co dalej?

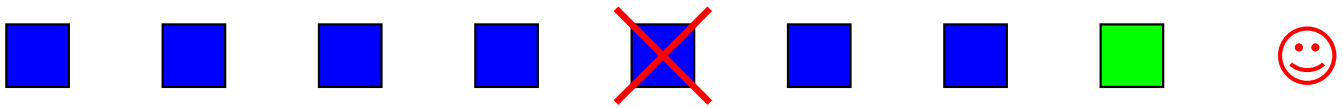
Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków
(na przykład nastąpi awaria któregoś z dysków)

Co dalej?

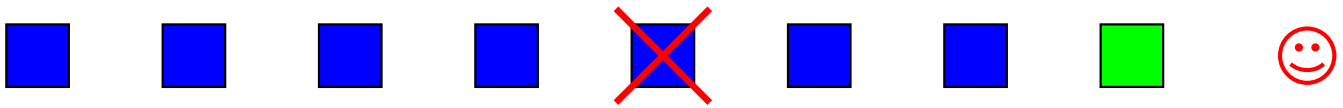
Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków (na przykład nastąpi awaria któregoś z dysków) to i tak jesteśmy w stanie odtworzyć wszystkie dane.

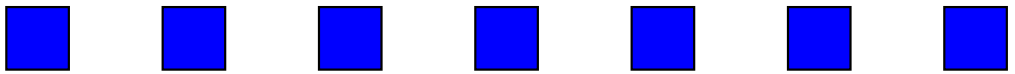
Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków (na przykład nastąpi awaria któregoś z dysków) to i tak jesteśmy w stanie odtworzyć wszystkie dane.

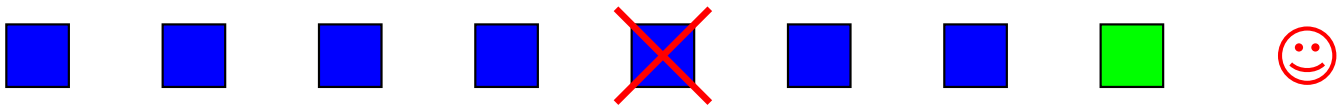
A czy można tak?:



Mamy dane w n kawałkach (na przykład na n dyskach).

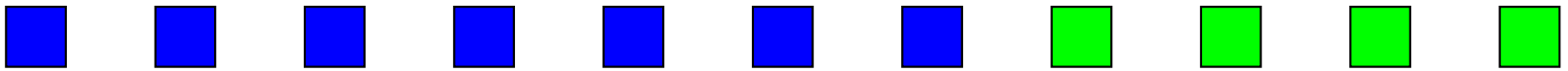
Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków (na przykład nastąpi awaria któregoś z dysków) to i tak jesteśmy w stanie odtworzyć wszystkie dane.

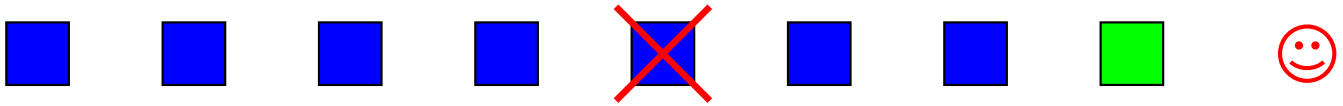
A czy można tak?:



Mamy dane w n kawałkach (na przykład na n dyskach).
„Dorabiamy” jeszcze m dodatkowych kawałków.

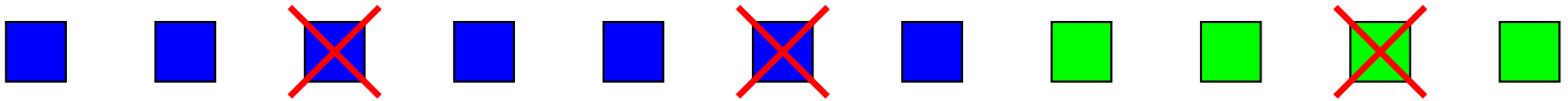
Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków (na przykład nastąpi awaria któregoś z dysków) to i tak jesteśmy w stanie odtworzyć wszystkie dane.

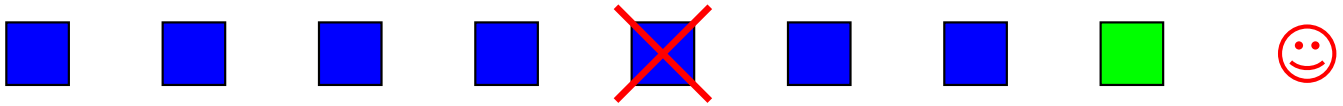
A czy można tak?:



Mamy dane w n kawałkach (na przykład na n dyskach).
„Dorabiamy” jeszcze m dodatkowych kawałków.
Chcielibyśmy móc odtworzyć nasze dane, jeśli stracimy dowolne $d \leqslant m$ kawałków naszych danych.

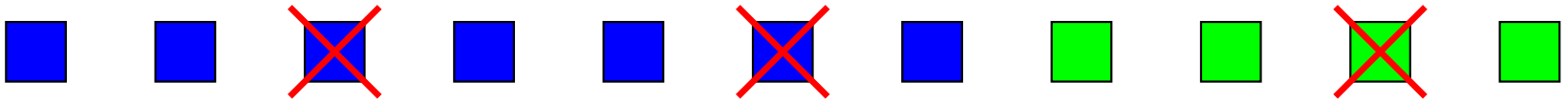
Co dalej?

Co nam dały krasnoludki (zwłaszcza krasnoludki I - bit parzystości)?



Mamy dane w n kawałkach (na przykład na n dyskach).
Możemy „dorobić” jeszcze jeden dodatkowy kawałek (razem mamy ich $n + 1$) tak, że jeśli stracimy dowolny z tych kawałków (na przykład nastąpi awaria któregoś z dysków) to i tak jesteśmy w stanie odtworzyć wszystkie dane.

A czy można tak?:



Mamy dane w n kawałkach (na przykład na n dyskach).
„Dorabiamy” jeszcze m dodatkowych kawałków.
Chcielibyśmy móc odtworzyć nasze dane, jeśli stracimy dowolne $d \leqslant m$ kawałków naszych danych.

Można: Algorytm Reeda–Solomola

Macierz Vandermonde'a

Niech K – ciało oraz $x_1, x_2, \ldots, x_n \in K$
Macierz Vandermonde'a to macierz kwadratowa

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

Macierz Vandermonde'a

Niech K – ciało oraz $x_1, x_2, \ldots, x_n \in K$
Macierz Vandermonde'a to macierz kwadratowa

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

Gdy $x_1, x_2, \ldots, x_n$ są parami różne, to jest ona odwracalna, bo $\det V = \prod_{i<j}(x_j - x_i)$

Macierz Vandermonde'a

Niech K – ciało oraz $x_1, x_2, \ldots, x_n \in K$
Macierz Vandermonde'a to macierz kwadratowa

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

Gdy $x_1, x_2, \ldots, x_n$ są parami różne, to jest ona odwracalna, bo $\det V = \prod_{i<j}(x_j - x_i)$

Inaczej: $V \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} P(x_1) \\ P(x_2) \\ \vdots \\ P(x_n) \end{pmatrix}$, gdzie $P(x) = a_1 + a_2 x + \cdots + a_n x^{n-1}$ jest wielomianem stopnia mniejszego od n. Zatem $V \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

oznacza, że P ma n różnych pierwiastków, a więc $P \equiv 0$, czyli $a_1 = a_2 = \cdots = a_n = 0$

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne. Rozważmy macierz $k \times n$

$$W = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ 1 & x_5 & x_5^2 & \cdots & x_5^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ 1 & x_{k-1} & x_{k-1}^2 & \cdots & x_{k-1}^{n-1} \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix}$$

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne. Rozważmy macierz $k \times n$

$$W = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix}$$

Jeżeli wykreślimy w macierzy W dowolne liczbę wierszy tak, by zostało tylko n wierszy, to dostaniemy macierz Vandermonde'a (odwracalną).

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne. Rozważmy macierz $k \times n$

$$W = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ \blacksquare & \blacksquare & \blacksquare & \blacksquare & \blacksquare \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix}$$

Jeżeli wykreślimy w macierzy W dowolne liczbę wierszy tak, by zostało tylko n wierszy, to dostaniemy macierz Vandermonde'a (odwracalną).

Wniosek: Jeśli dla pewnych $a_1, \ldots, a_n \in K$ wyznaczymy $b_1, \ldots, b_k$ $(b_1, \ldots, b_k)^T = W(a_1, \ldots, a_n)^T$ i jeśli stracimy (zapomnimy) część spośród b_j, ale tak, że zostanie nam co najmniej n spośród b_j (i będziemy wiedzieć które), to będziemy mogli odtworzyć $a_1, \ldots, a_n$.

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne. Rozważmy macierz $k \times n$

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$$

Wniosek: Jeśli dla pewnych $a_1, \ldots, a_n \in K$ wyznaczymy $b_1, \ldots, b_k$ $(b_1, \ldots, b_k)^T = W(a_1, \ldots, a_n)^T$ i jeśli stracimy (zapomnimy) część spośród b_j, ale tak, że zostanie nam co najmniej n spośród b_j (i będziemy wiedzieć które), to będziemy mogli odtworzyć $a_1, \ldots, a_n$.

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne.
Rozważmy macierz $k \times n$

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ \vdots \\ b_{k-2} \\ b_{k-1} \\ b_k \end{pmatrix} = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ 1 & x_5 & x_5^2 & \cdots & x_5^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ 1 & x_{k-1} & x_{k-1}^2 & \cdots & x_{k-1}^{n-1} \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$$

Wniosek: Jeśli dla pewnych $a_1, \ldots, a_n \in K$ wyznaczymy $b_1, \ldots, b_k$ $(b_1, \ldots, b_k)^T = W(a_1, \ldots, a_n)^T$ i jeśli stracimy (zapomnimy) część spośród b_j, ale tak, że zostanie nam co najmniej n spośród b_j (i będziemy wiedzieć które), to będziemy mogli odtworzyć $a_1, \ldots, a_n$.

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne.
Rozważmy macierz $k \times n$

$$\begin{pmatrix} b_1 \\ \blacksquare \\ \blacksquare \\ b_4 \\ \blacksquare \\ \vdots \\ b_{k-2} \\ \blacksquare \\ b_k \end{pmatrix} = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \cdots & x_3^{n-1} \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ 1 & x_5 & x_5^2 & \cdots & x_5^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ 1 & x_{k-1} & x_{k-1}^2 & \cdots & x_{k-1}^{n-1} \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$$

Wniosek: Jeśli dla pewnych $a_1, \ldots, a_n \in K$ wyznaczymy $b_1, \ldots, b_k$ $(b_1, \ldots, b_k)^T = W(a_1, \ldots, a_n)^T$ i jeśli stracimy (zapomnimy) część spośród b_j, ale tak, że zostanie nam co najmniej n spośród b_j (i będziemy wiedzieć które), to będziemy mogli odtworzyć $a_1, \ldots, a_n$.

Użycie macierzy Vandermonde'a

Niech teraz $k \geqslant n$ oraz niech $x_1, x_2, \ldots, x_k \in K$ – parami różne.
Rozważmy macierz $k \times n$

$$\begin{pmatrix} b_1 \\ \\ \\ b_4 \\ \\ \vdots \\ b_{k-2} \\ \\ b_k \end{pmatrix} = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \\ \\ 1 & x_4 & x_4^2 & \cdots & x_4^{n-1} \\ \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{k-2} & x_{k-2}^2 & \cdots & x_{k-2}^{n-1} \\ \\ 1 & x_k & x_k^2 & \cdots & x_k^{n-1} \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix}$$

Wniosek: Jeśli dla pewnych $a_1, \ldots, a_n \in K$ wyznaczymy $b_1, \ldots, b_k$ $(b_1, \ldots, b_k)^T = W(a_1, \ldots, a_n)^T$ i jeśli stracimy (zapomnimy) część spośród b_j, ale tak, że zostanie nam co najmniej n spośród b_j (i będziemy wiedzieć które), to będziemy mogli odtworzyć $a_1, \ldots, a_n$.

Problem: Potrzebujemy ciała K, które ma sporo elementów, a $\mathbb{Z}_2$ ma tylko dwa elementy. Co zrobić?

Problem: Potrzebujemy ciała K, które ma sporo elementów, a $\mathbb{Z}_2$ ma tylko dwa elementy. Co zrobić?

Sproduktować ciało $\mathbb{Z}_2$ dostając $\mathbb{Z}_2^r$!

Problem: Potrzebujemy ciała K, które ma sporo elementów, a $\mathbb{Z}_2$ ma tylko dwa elementy. Co zrobić?

~~Sproduktować ciało $\mathbb{Z}_2$ dostając $\mathbb{Z}_2^r$!~~ Produkt ciał nie jest ciałem. W $\mathbb{Z}_2^r$ dodawanie jest dobre, ale mnożenie jest złe. Co zrobić?

Problem: Potrzebujemy ciała K, które ma sporo elementów, a $\mathbb{Z}_2$ ma tylko dwa elementy. Co zrobić?

~~Sproduktować ciało $\mathbb{Z}_2$ dostając $\mathbb{Z}_2^r$!~~ Produkt ciał nie jest ciałem. W $\mathbb{Z}_2^r$ dodawanie jest dobre, ale mnożenie jest złe. Co zrobić?

Należy wybrać wielomian $W \in \mathbb{Z}_2[x]$ stopnia r nierozkładalny nad $\mathbb{Z}_2$. Następnie, każdy element $\mathbb{Z}_2^r$ utożsamiamy z wielomianem stopnia mniejszego niż r:
$(z_1, z_2, \ldots, z_r) \leftrightsquigarrow z_r x^{r-1} + z_{r-1} x^{r-2} + \cdots + z_1$.
Mnożenie i dodawanie w $\mathbb{Z}_2^r$ to mnożenie i dodawanie wielomianów modulo W. W ten sposób dostajemy ciało skończone mające 2^r elementów.

Problem: Potrzebujemy ciała K, które ma sporo elementów, a $\mathbb{Z}_2$ ma tylko dwa elementy. Co zrobić?

~~Sproduktować ciało $\mathbb{Z}_2$ dostając $\mathbb{Z}_2^r$!~~ Produkt ciał nie jest ciałem. W $\mathbb{Z}_2^r$ dodawanie jest dobre, ale mnożenie jest złe. Co zrobić?

Należy wybrać wielomian $W \in \mathbb{Z}_2[x]$ stopnia r nierozkładalny nad $\mathbb{Z}_2$. Następnie, każdy element $\mathbb{Z}_2^r$ utożsamiamy z wielomianem stopnia mniejszego niż r:
$(z_1, z_2, \ldots, z_r) \leftrightsquigarrow z_r x^{r-1} + z_{r-1} x^{r-2} + \cdots + z_1$.
Mnożenie i dodawanie w $\mathbb{Z}_2^r$ to mnożenie i dodawanie wielomianów modulo W. W ten sposób dostajemy ciało skończone mające 2^r elementów.

Używając tak skonstruowanych ciał skończonych i wcześniejszych obserwacji związanych z macierzą Vandermonde'a dostajemy algorytm Reeda–Solomona.