Cap Conjecture - motywacje i zastosowania

Weronika Lorenczyk

28 stycznia 2021

problem CAP

Twierdzenie (CAP)

Największy podzbiór $(\mathbb{Z}/3\mathbb{Z})^n$, który nie zawiera ciągu arytmetycznego długości 3 jest co najwyżej rozmiaru c^n, dla pewnego ustalonego $c < 3$.

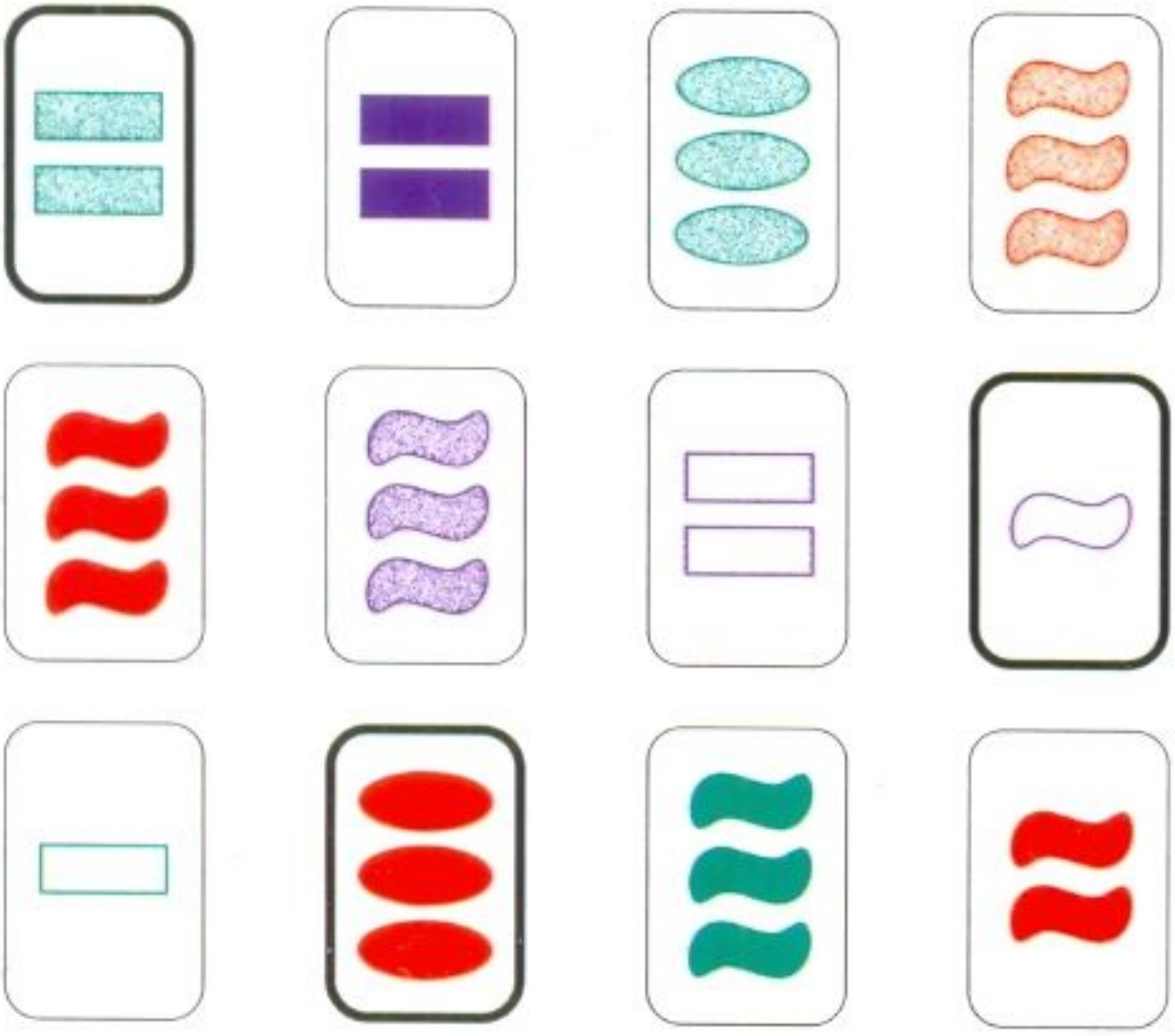
Dowód problemu CAP

- W 2016 Croot, Lev, i Pach rozwiązali analogiczny problem dla $(\mathbb{Z}/4\mathbb{Z})^n$
- Niedługo potem Ellenberg i Gijswijt dopracowali wcześniejszy dowód i rozwiązali oryginalny problem
- Dowód jest dość elementarny i krótki, jednak hipoteza była otwarta przez długi czas

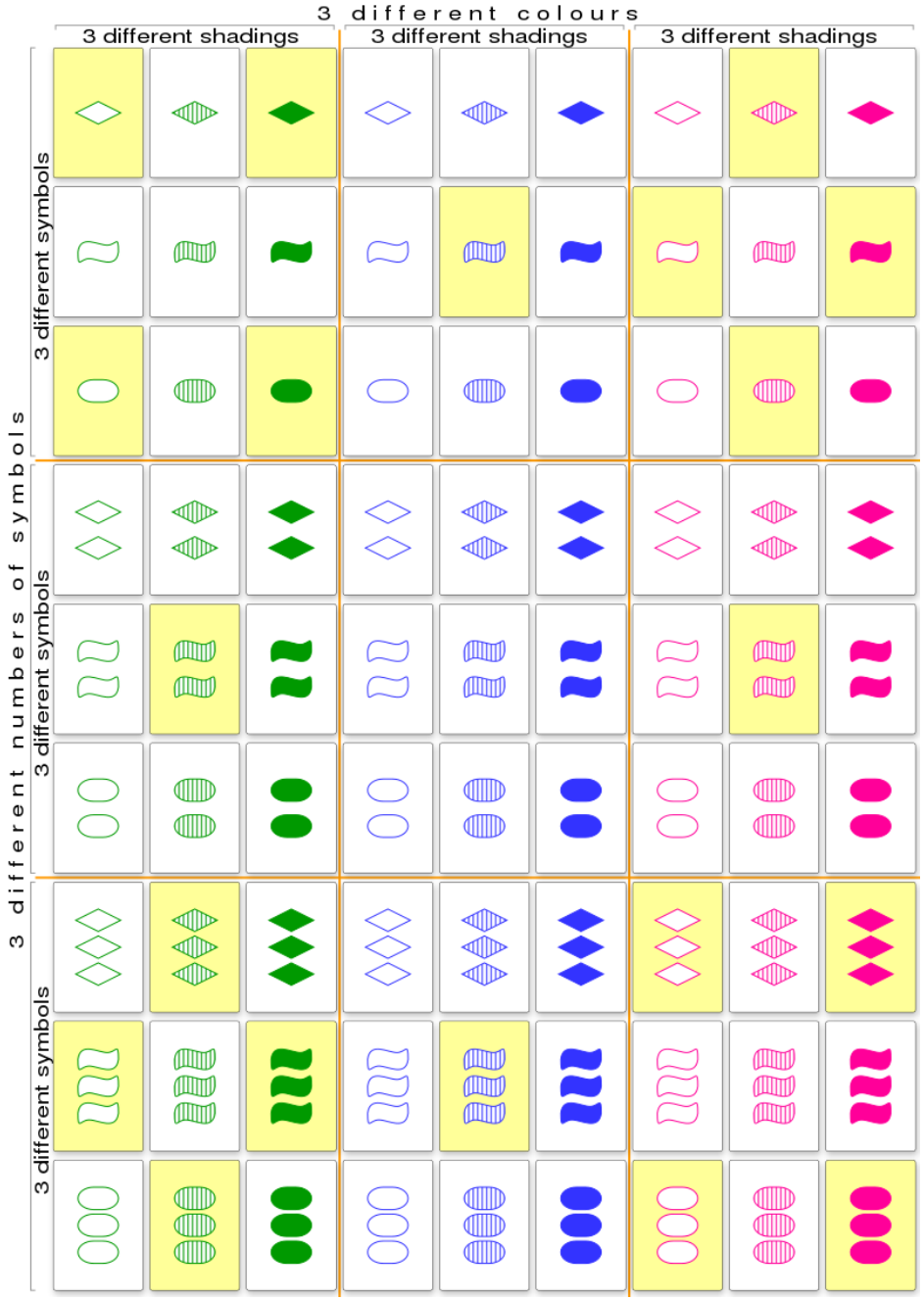
Intuicje

W $(\mathbb{Z}/3\mathbb{Z})^n$ ciągiem arytmetycznym długości 3 będą liczby x, y, z takie, że $x + y = 2z$, albo równoważnie $x + y + z = 0(mod\ 3)$.
W tym zbiorze nie istnieje ciąg arytmetyczny dłuższy niż 3. Dla $a, a + b, a + 2b, a + 3b$, wiemy że $a = a + 3b$

Gra SET



Największy zbiór bez SETów



Struktury addytywne i multiplikatywne

- **Addytywne** Liczby naturalne można przedstawić jako $1 + 1 + \cdots$. W tej reprezentacji łatwo możemy dodawać, ale trudno mnożyć czy znaleźć rozkład.
- **Multiplikatywne** Liczby można też przedstawić jako iloczyn liczb pierwszych. Łatwe mnożenie, trudne dodawanie.
- Na liczby naturalne możemy patrzeć z dwóch perspektyw

Zależność między strukturami

Czasem patrzymy się na obydwie struktury na raz. Tworzy to pytania:

- Jaka jest różnica pomiędzy kolejnymi liczbami pierwszymi?
- Jaka jest relacja pomiędzy rozkładem n i n+1?

Wiedza współczesna

Pytania które zadajemy są bardzo proste i podstawowe, ale jest w nich dużo do odkrycia. Dopiero w 2013 udowodniono, że istnieje nieskończenie wiele par liczb pierwszych o różnicy mniejszej od pewnej stałej c. Udało się nam obniżyć c jedynie do 246.

Liczby pierwsze bliźniacze

Definicja (liczby bliźniacze)

Liczby pierwsze różniące się o 2. Przykłady to 5 i 7, 11 i 13

Twierdzenie (Hipoteza liczb bliźniaczych)

Istnieje nieskończenie wiele liczb bliźniaczych

Rozbudowywanie problemu

Zamiast na różnice pomiędzy kolejnymi liczbami pierwszymi możemy patrzeć na zbudowane z nich ciągi arytmetyczne. Przez ponad 200 lat próbowano udowodnić, że liczby pierwsze zawierają ciągi arytmetyczne dowolnej długości. Green i Tao przedstawili dowód w 2004 roku.

Rozbudowywanie problemu

Chociaż pytania nasuwają się same na wiele z nich nie znamy odpowiedzi. Prawie 70 lat przed twierdzeniem Greena-Tao pokazano, że istnieje nieskończenie wiele ciągów arytmetycznych długości 3. Ale istnienie nieskończenie wielu ciągów długości 4, czy nawet jednego długości 24 zostało nieudowodnione wcześniej w innych publikacjach.

Łatwiejszy setting

Zamiast zajmować się liczbami naturalnymi uprośćmy sobie życie na chwilkę i rozważmy inną grupę abelową. To najprostszy zbiór w którym możemy mówić o strukturze addytywnej. Natychmiastowym wyborem zdaje się $\mathbb{Z}/m\mathbb{Z}$. Aby zapewnić sobie możliwość rozszerzania o nowe elementy dodamy $(\mathbb{Z}/m\mathbb{Z})^n$

Czy nie zmieniliśmy problemu za bardzo?

Okazuje się, że tego typu rozważania mogą być jak najbardziej pomocne. Istnieją metody przenoszenia rezultatów pomiędzy różnymi grupami abelowymi. Najlepszym przykładem jest homomorfizm Freimana.

Definicje

Definicja (Zbiór addytywny)

Zbiorem addytywnym A nazywany podzbiór grupy abelowej Z

Definicja (Struktura k-addytywna)

Jest ona zdefiniowana przez wszystkie wyrażenia
$a_1 + \cdots + a_k = b_1 + \cdots + b_k,\ a_i, b_i \in A$

Ciąg arytmetyczny będzie strukturą 2-addytywną zdefiniowaną przez wyrażenia postaci $a_i + a_{i+2} = a_{i+1} + a_{i+1}$

Homomorfizm Freimana

Definicja (Homomorfizm Freimana)

k-homomorfizm Freimana pomiędzy zbiorami addytywnymi $A \in Z$ *i* $B \in W$ *to funkcja z A do B, która dla każdych* $a_i, b_i \in A$

$$a_1 + \cdots + a_k = b + 1 + \cdots + b_k \Rightarrow f(a_1) + \cdots + f(a_k) = f(b_1) + \cdots + f(b_k)$$

Nie jest on w stanie przenieść wyników z naszych skończonych zbiorów w nieskończony $\mathbb{Z}$, ale może w tym bardzo pomóc

Proste ograniczenia dolne

Zastanówmy się jak prosto skonstruować ograniczenia dolne. Dla $n = 1$ przykładem będzie $\{0, 1\}$ - zbiór wielkości 2^1. Dla większych n, zadziała jego rozszerzenie $\{0, 1\}^n$. Analogicznie jeżeli znajdziemy ograniczenie rozmiaru c dla pewnego d, mamy ograniczenie $c^{n/d}$ dla wymiaru n. Najlepsze znane ograniczenia zostały skonstruowane tą metodą.

Czego jeszcze nie wiemy

Nawet w czystym problemie sat istnieje jeszcze wykładnicza różnica pomiędzy ograniczeniem górnym 2.756^n i dolnym 2.217^n i pozbycie się jej jest ciekawym zadaniem. Do poprawienia dolnego ograniczenia wystarczyłaby jedna dobra konstrukcja.

Podsumowanie