Podciągi

Radosław Żak

Streszczenie

W pracy badamy własności funkcji zliczającej podciągi danego słowa.

1 Wprowadzenie. Konwencje

> Nie zaszkodzi, ale też niewiele pomoże, parę słów przedmowy.
>
> ---
>
> „Tumor Mózgowicz”
> Stanisław Ignacy Witkiewicz

W poniższej pracy będziemy badać własności liczby podciągów danego słowa. W rozdziale drugim wprowadzimy podstawowe pojęcia z tym związane. Zakres dalszych rozważań jest dosyć rozległy – w rozdziale trzecim przyjrzymy się tym zagadnieniom z perspektywy teorii liczb, przedstawiając przy tym dowód klasycznego twierdzenia Fermata o sumie dwóch kwadratów. W rozdziale czwartym zastanowimy się, jak krótkie słowa o N różnych podciągach możemy znaleźć, pokazując, że długość ta będzie $O(\log N)$ dla N w zbiorze gęstości 1. Następnie przechodzimy do badania trajektorii funkcji $\mathsf{P} : \mathbb{N} \to \mathbb{N}$, która liczbie naturalnej przyporządkuje liczbę jej podciągów w ustalonym zapisie liczbowym. Po rozstrzygnięciu tych kwestii w systemach pozycyjnych rozważamy je w systemie Zeckendorfa, wprowadzając także równoważność liczby podciągów i macierzy. W dodatkach przedstawiamy wyjątkowo mało koncepcyjne dowody, oraz problemy otwarte jakie w naturalny sposób można postawić w kontekście poniższej pracy.

Przez $\mathcal{M}_k$ będziemy oznaczali zbiór słów nad alfabetem złożonym z k elementów (dobór alfabetu będzie wynikał z kontekstu). Razem z konkatenacją, oznaczaną tu przez $\star$, zbiór ten będzie monoidem, w którym słowo puste, oznaczane przez $\mathsf{0}$, będzie elementem neutralnym. W naturalny sposób wprowadzamy tu potęgowanie – A^n jest słowem składającym się z n liter A. Długość słowa $\mathfrak{s}$ będziemy oznaczali przez $|\mathfrak{s}|$.

Przez ϕ będziemy oznaczali złotą liczbę równą $\frac{1+\sqrt{5}}{2}$, zaś przez F_n n-tą liczbę Fibonacciego ($F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$). Oznaczenie φ w zależności od kontekstu będzie funkcją Eulera lub stałą równą $\phi^{-1} = \phi - 1$.

Dla wygody będziemy przyjmowali $0 \notin \mathbb{N}$.

2 Podstawy i historia problemu

> Mówię jako laik, ale bądź co bądź laik długoletni.
>
> „Czarodziejska góra"
> Tomasz Mann

Na I etapie XXVI Olimpiady Informatycznej pojawiło się następujące zadanie[1]:

Zadanie. Dana jest liczba naturalna $N \leqslant 10^{18}$. Wypisz słowo, które ma dokładnie N różnych podciągów i co najwyżej 1000 znaków.

Dla przykładu słowo ABA ma siedem różnych podciągów: $\mathsf{0}$, A, B, AA, AB, BA oraz całe słowo.

Zarys rozwiązania wzorcowego. Niech $\mathsf{P}(\mathfrak{s})$ oznacza liczbę podciągów słowa $\mathfrak{s}$. Jeśli $\mathfrak{s}$ nie zawiera litery A, to

$$\mathsf{P}(\mathsf{A}^k \star \mathfrak{s} \star \mathsf{A}^l) = (k+1)(l+1)(\mathsf{P}(\mathfrak{s}) - 1) + (k+l+1),$$

istotnie, albo w podciągu wystąpią jakieś litery różne od A – wtedy wybieramy podciąg z $\mathfrak{s}$ na $\mathsf{P}(\mathfrak{s})-1$ sposobów, oraz liczbę liter A z lewej i z prawej strony na $(k+1)(l+1)$ sposobów; albo takowe nie wystąpią, i wybieramy liczbę A na $k+l+1$ sposobów. W ten sposób, jeśli $(k+1)(l+1) \mid N-(k+l+1)$, możemy sprowadzić problem szukania słowa o N podciągach do problemu szukania słowa o $\frac{1}{(k+1)(l+1)}(N-k-l-1)+1$, podciągach. Okazuje się, że wypisanie wszystkich takich zależności dla względnie niewielkich k, l daje wystarczająco by sytuacja dla dowolnego N dawała się w taki sposób zredukować; po wystarczająco wielu takich redukcjach dochodzimy do przypadku $N = 1$, i wtedy nasz proces możemy zakończyć.

Moje rozwiązanie było jednak znacząco inne:

[1] Pozwoliłem sobie zignorować informatyczną część otoczki, i zostawić samo wnętrze.

Definicja 2.1. Dla dwóch względnie pierwszych liczb $a,\ b \geqslant 1$ przez $\mathrm{gen}(a, b)$ będziemy konstruowali rekurencyjnie słowo:

$$\mathrm{gen}(a,b) = \begin{cases} \mathsf{0},\ \text{jeśli } a = b = 1, \\ \mathsf{A} \star \mathrm{gen}(a-b, b), & \text{jeśli } a > b \\ \mathsf{B} \star \mathrm{gen}(a, b-a), & \text{jeśli } b > a \end{cases}$$

Słowo to jest w pewnym sensie zapisem algorytmu Euklidesa dla liczb $a,\ b$ – w każdym momencie zapisujemy od której z liczb jest odejmowana druga (i właśnie prawdziwość algorytmu Euklidesa dowodzi, że $\mathrm{gen}(a, b)$ jest dobrze określony). Okazuje się, że słowa te mają zaskakującą w kontekście naszych rozważań własność.

Twierdzenie 2.1. $\mathsf{P}(\mathrm{gen}(a, b)) = a + b - 1$

Zanim przejdziemy do dowodu, wprowadzimy jeszcze przydatną definicję.

Definicja 2.2. Będziemy oznaczać liczbę podciągów $\mathfrak{s}$ zaczynających się od (kończących się na) A przez $\mathsf{P}^{\mathsf{A}}(\mathfrak{s})$ ($\mathsf{P}_{\mathsf{A}}(\mathfrak{s})$). Podobnie definiujemy analogiczne wyrażenia dla B. Będziemy też łączyć te oznaczenia: dla przykładu $\mathsf{P}^{\mathsf{B}}_{\mathsf{A}}(\mathfrak{s})$ jest liczbą podciągów $\mathfrak{s}$ postaci $\mathsf{B} \ldots \mathsf{A}$.

Uwaga. Podciąg pusty wliczamy do wszystkich wyrażeń powyższej postaci **oprócz** $\mathsf{P}^{\mathsf{A}}_{\mathsf{A}}$ i $\mathsf{P}^{\mathsf{B}}_{\mathsf{B}}$. Dokładne powody takiego wyboru zobaczymy później, warto jednak zauważyć że w ten sposób zachodzi $\mathsf{P}_{\mathsf{A}}(\mathfrak{s}) = \mathsf{P}^{\mathsf{A}}_{\mathsf{A}}(\mathfrak{s}) + \mathsf{P}^{\mathsf{B}}_{\mathsf{A}}(\mathfrak{s})$ oraz symetryczne równości, a także $\mathsf{P}(\mathfrak{s}) = \mathsf{P}_{\mathsf{A}}(\mathfrak{s}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{s}) - 1$ (gdzie -1 wynika z podwójnego policzenia $\mathsf{0}$).

Dowód. Będziemy chcieli indukcyjnie pokazać, że $\mathsf{P}^{\mathsf{A}}(\mathrm{gen}(a, b)) = a$ (oraz analogicznie $\mathsf{P}^{\mathsf{B}}(\mathrm{gen}(a, b)) = b$): to razem ze wzorem z uwagi wyżej da nam tezę. Dla $a = b = 1$ w obu tych wyrażeniach jedynym wliczanym podciągiem jest $\mathsf{0}$.

Jeśli $a < b$, to pierwszą literą $\mathrm{gen}(a, b)$ jest B. Oczywiście nie może ona wchodzić w skład żadnego podciągu rozpoczynającego się od A, więc podciągów tych będzie, co po usunięciu tej litery – pozostałą częścią słowa jest zaś $\mathrm{gen}(a, b - a)$, więc z założenia indukcyjnego teza działa.

Pozostaje przypadek $a > b$. Wtedy pierwszą literą naszego słowa jest A. Zauważmy, że wybierając litery do dowolnego podciągu zaczynającego się od A możemy rozpocząć go tą samą literą od której zaczyna się całe słowo – w ten sposób pozostałe litery będą stanowić jakiś podciąg pozostałej części słowa; widzimy więc że zbiór naszych podciągów jest równoliczny ze zbiorem wszystkich podciągów słowa powstałego po usunięciu pierwszej litery A.

Musimy jeszcze uwzględnić to, że także $\mathsf{0}$ zaczyna się od A, więc ostatecznie $\mathsf{P}^{\mathsf{A}}(\mathrm{gen}(a,b)) = \mathsf{P}(\mathrm{gen}(a-b,b))+1 = ((a-b)+b-1)+1 = a$, co chcieliśmy udowodnić. □

Przykład. Weźmy $a = 11$, $b = 7$. Wtedy $\mathrm{gen}(11,7) = \mathsf{A} \star \mathrm{gen}(4,7) = \mathsf{AB}\star\mathrm{gen}(4,3) = \mathsf{ABA}\star\mathrm{gen}(1,3) = \mathsf{ABAB}\star\mathrm{gen}(1,2) = \mathsf{ABABB}$. Bezpośrednio możemy sprawdzić, że ABABB ma 10 niepustych podciągów zaczynających się od A oraz 6 zaczynających się od B.

Korzystając z Twierdzenia 2.1, potrafimy w prosty sposób wygenerować słowo o dokładnie N podciągach, i to zawierające tylko dwie różne litery: wystarczy dobrać a dla którego $\mathrm{nwd}(a, N+1) = 1$ i wypisać $\mathrm{gen}(a, N+1-a)$. Problemem może się okazać długość takiego słowa – w praktyce kombinacja dobrania $a \approx \frac{N+1}{\phi}$ z metodą prób i błędów dawała wystarczająco dobre rezultaty z informatycznego punktu widzenia. Wrócimy do tego tematu w rozdziale czwartym, gdzie udowodnimy że dla dowolnego N znajdziemy takie słowo o długości $O(\sqrt{N})$ – wydaje się jednak, że jest to rezultat daleki od optymalnego.

Z dowodu powyższego twierdzenia wynika także, że funkcją odwrotną do gen jest $\mathfrak{s} \to \big((\mathsf{P}^{\mathsf{A}}(\mathfrak{s}), \mathsf{P}^{\mathsf{B}}(\mathfrak{s})\big)$, co daje przydatną bijekcję między elementami $\mathcal{M}_2$ a parami względnie pierwszych liczb naturalnych.

3 Liczby i symetrie

> Aby walczyć z abstrakcją, trzeba być trochę do niej podobnym.
>
> „Dżuma”
> Albert Camus

W tym rozdziale opiszemy niektóre własności funkcji gen powiązane z symetriami słów. Zacznijmy od prostego wniosku z Twierdzenia 1:

Fakt 3.1. Istnieje $\varphi(N+1)$ słów o N podciągach w $\mathcal{M}_2$.

Dowód. Wszystkie takie słowa są postaci $\mathrm{gen}(a,b)$, gdzie $a+b = N+1$ oraz $\mathrm{nwd}(a,b) = 1$. Takich par jest tyle ile możemy dobrać a względnie pierwszych z $N+1$ (gdyż $\mathrm{nwd}(a, N+1) = \mathrm{nwd}(a, N+1-a) = \mathrm{nwd}(a,b)$), czyli dokładnie $\varphi(N+1)$. □

W ten sposób możemy utożsamić słowa[2] o N podciągach z elementami zbioru $\mathbb{Z}_{N+1}^{\times}$. Ponieważ w naszych rozważaniach N nie będzie się pojawiało „samodzielnie”, podstawmy $M := N + 1$.

Dla słowa $\mathfrak{s}$ zdefiniujemy przez $\mathfrak{s}^*$ słowo powstałe przez zamianę wszystkich liter A na B i *vice versa*, przez $\overline{\mathfrak{s}}$ odwrócenie słowa $\mathfrak{s}$, zaś przez $\widetilde{\mathfrak{s}}$ połączenie tych dwóch operacji. Zauważmy, że każda z tych operacji jest odwrotna do samej siebie. Do tego działa ona jednocześnie w ten sam sposób na wszystkich swoich podciągach, toteż $\mathsf{P}(\mathfrak{s}) = \mathsf{P}(\mathfrak{s}^*) = \mathsf{P}(\overline{\mathfrak{s}}) = \mathsf{P}(\widetilde{\mathfrak{s}})$. Symetrie słów muszą więc odpowiadać jakimś symetriom $\mathbb{Z}_M^{\times}$ – zbadamy zatem, jakim.

Lemat 3.1. $\mathsf{P}^{\mathsf{A}}(\mathfrak{s}^*) = M - \mathsf{P}^{\mathsf{A}}(\mathfrak{s})$

Dowód. W zmianie $\mathfrak{s} \to \mathfrak{s}^*$ podciągi zaczynające się od A przekształcą się w podciągi zaczynające się od B, stąd otrzymujemy tezę. □

Twierdzenie 3.1.
$$\mathsf{P}^{\mathsf{A}}(\mathfrak{s})\mathsf{P}^{\mathsf{A}}(\overline{\mathfrak{s}}) \equiv 1 \pmod{M}$$

Dowód. Oczywiście równoważnie możemy zapisać tezę jako $\mathsf{P}^{\mathsf{A}}(\mathfrak{s})\mathsf{P}_{\mathsf{A}}(\mathfrak{s}) \equiv 1 \pmod{M}$. Oznaczmy $a = \mathsf{P}^{\mathsf{A}}(\mathfrak{s})$ oraz $b = M - a$, wtedy $\mathfrak{s} = \mathrm{gen}(a, b)$.

Niech $t = |s|$. Będziemy budować ciąg macierzy $M_k = \begin{pmatrix} c_k & d_k \\ e_k & f_k \end{pmatrix}$, w ten sposób, że po k krokach algorytmu Euklidesa para (a, b) stanie się równa $(c_k a + d_k b, e_k a + f_k b)$. Zatem na początku $c_0 = f_0 = 1$ oraz $d_0 = e_0 = 0$. Jeśli k-ta litera to A, dostajemy:

- $e_k = e_{k-1}$, $f_k = f_{k-1}$
- $c_k = c_{k-1} - e_{k-1}$, $d_k = d_{k-1} - f_{k-1}$

Jeśli teraz utworzymy ciągi $x_k = c_k - d_k$, $y_k = f_k - e_k$, w powyższym przypadku będziemy mieli $y_k = y_{k-1}$ oraz $x_k = x_{k-1} + y_{k-1}$. Zatem para (x_k, y_k) zmienia się tak jakby był przeprowadzany algorytm Euklidesa – ale w drugą stronę ($(x_0, y_0) = (1, 1)$). Zatem $\mathfrak{s} = \overline{\mathrm{gen}(x_t, y_t)}$. Wiemy ponadto, że algorytm kończy się na parze $(1, 1)$, więc $c_t a + d_t b = 1$. Ponieważ $b \equiv -a \pmod{M}$, mamy $x_t a = (c_t - d_t)a \equiv c_t a + d_t b = 1 \pmod{M}$, co chcieliśmy udowodnić.

□

Twierdzenie 3.1 pokazuje, że odwzorowanie $\mathfrak{s} \mapsto \overline{\mathfrak{s}}$ odpowiada $a \mapsto a^{-1}$ w $\mathbb{Z}_M^{\times}$ – odwracanie w znaczeniu „lingwistycznym” okazuje się być tym samym, co w znaczeniu liczbowym.

[2] Będziemy od teraz rozważać tylko słowa z $\mathcal{M}_2$.

Definicja 3.1. Słowo $\mathfrak{s}$ nazwiemy *palindromem*, jeśli $\mathfrak{s} = \overline{\mathfrak{s}}$, oraz *antypalindromem*, jeśli $\mathfrak{s} = \widetilde{\mathfrak{s}}$.

Oznaczmy przez $\omega(n)$ liczbę różnych dzielników pierwszych liczby n.

Fakt 3.2. Palindromów o $M-1$ podciągach jest $2^{\omega(M)-1}$, gdy $M \equiv 2 \pmod 4$, $2^{\omega(M)+1}$ gdy $8|M$, oraz $2^{\omega(M)}$ w innych przypadkach.

Sformułowanie powyższego faktu może wydawać się skomplikowane, ale ogólna zasada jest prosta: każdy nieparzysty dzielnik pierwszy mnoży liczbę palindromów razy dwa, potęgi dwójki zaś będą się zachowywać nieco dziwniej.

Dowód. Z Twierdzenia 3.1 wiemy, że każdy z tych palindromów to słowo $\mathrm{gen}(a, M-a)$, gdzie a spełnia zależność $a \equiv a^{-1} \pmod M$, czyli $a^2 \equiv 1 \pmod M$. Z chińskiego twierdzenia o resztach, każde rozwiązanie tej kongruencji odpowiada jakiemuś wyborowi jej rozwiązań modulo dzielniki M będące potęgami liczb pierwszych. Chcemy więc zbadać, ile wynosi liczba tych rozwiązań dla $M = p^k$.

Gdy $2 \nmid p$, mamy $a^2 - 1 \equiv 0 \pmod{p^k}$, a więc $p^k \mid (a-1)(a+1)$. Skoro $p > 2$, zaś $\mathrm{nwd}(a-1, a+1) \leqslant |(a+1)-(a-1)| = 2$, to co najmniej jeden z czynników tego iloczynu jest względnie pierwszy z p, pozostały więc musi być podzielny przez p^k. Zatem $a \equiv \pm 1 \pmod{p^k}$, otrzymujemy dwa rozwiązania.

Dla $p = 2$ ręcznie możemy sprawdzić, że mamy jedno rozwiązanie modulo 2, dwa modulo 4, oraz cztery modulo 8. Dla $k \geqslant 4$ zauważmy, że skoro $2^k \mid (a-1)(a+1)$, to a jest nieparzyste, zatem z podobnego argumentu co wcześniej jeden z tych czynników jest parzysty, ale niepodzielny przez 4, pozostały więc musi być podzielny przez 2^{k-1}. Są zatem cztery rozwiązania: $a \equiv \pm 1 \pmod{2^k}$ oraz $a \equiv 2^{k-1} \pm 1 \pmod{2^k}$.

Podsumowując wszystkie przypadki, dostajemy wzory jak w tezie. □

Fakt 3.3. Jeśli $M \mid 24$, to każde słowo o $M-1$ podciągach jest palindromem (i na odwrót).

Dowód. Z poprzedniego dowodu widzimy, że M spełnia tę własność wtedy i tylko wtedy, gdy każdy jego dzielnik będący potęgą liczby pierwszej także ją spełnia. Ponieważ dla nieparzystych potęg liczb pierwszych mamy tylko dwa palindromy, to jedynymi liczbami nieparzystymi które spełniają naszą własność są 1 i 3. Dla potęg dwójki zaś wiemy że te równe co najwyżej 8 spełniają naszą własność, zaś przy 2^k dla $k \geqslant 4$ mamy tylko cztery palindromy, czyli mniej niż wszystkich względnie pierwszych reszt (2^{k-1}). Stąd wnioskujemy, że istotnie $M \mid 24$. □

Przykład. Dla $N = 23$ otrzymujemy więc słowa A^{22}, $\mathsf{AAABAAA}$, AABBAA, $\mathsf{ABBBBBA}$, oraz analogiczne słowa po zamianach $\mathfrak{s} \mapsto \mathfrak{s}^*$.

Fakt 3.4. Słowo $\mathfrak{s}$ jest antypalindromem wtedy i tylko wtedy, gdy jest postaci $\mathfrak{s} = \mathfrak{t} \star \widetilde{\mathfrak{t}}$.

Dowód. Łatwo zauważyć, że każde słowo tej postaci jest antypalindromem – w ogólności $\widetilde{\mathfrak{t} \star \mathfrak{r}} = \widetilde{\mathfrak{r}} \star \widetilde{\mathfrak{t}}$, więc istotnie $\widetilde{\mathfrak{t} \star \widetilde{\mathfrak{t}}} = \mathfrak{t} \star \widetilde{\mathfrak{t}}$. Aby wykazać odwrotną implikację zauważmy, że jeśli $\mathfrak{s}$ jest antypalindromem, to musi mieć parzystą liczbę liter – istotnie, środkowa litera w naturalny sposób nie może istnieć. Biorąc zaś $\mathfrak{t}$ jako pierwszą połówkę $\mathfrak{s}$, otrzymujemy żądany rozkład. $\square$

Wiemy, że antypalindromy o $M - 1$ podciągach to takie $\mathrm{gen}(a, M - a)$, że $a^2 \equiv -1 \pmod{M}$. Z tej obserwacji wyprowadzimy znane twierdzenie Fermata o sumie dwóch kwadratów[3]. Najpierw jednak ważne twierdzenie charakteryzujące liczbę podciągów konkatenacji dwóch słów:

Twierdzenie 3.2.

$$\mathsf{P}(\mathfrak{s} \star \mathfrak{t}) = \mathsf{P}_{\mathsf{A}}(\mathfrak{s})\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{s})\mathsf{P}^{\mathsf{A}}(\mathfrak{t}) - 1$$

Dowód. Będziemy dowodzić indukcyjnie po długości $\mathfrak{s}$. Dla $\mathfrak{s} = \mathsf{0}$ teza jest oczywista. Bez straty ogólności $\mathfrak{s} = \mathfrak{r} \star \mathsf{A}$, wtedy $\mathsf{P}_{\mathsf{B}}(\mathfrak{s}) = \mathsf{P}_{\mathsf{B}}(\mathfrak{r})$ oraz $\mathsf{P}_{\mathsf{A}}(\mathfrak{s}) = \mathsf{P}_{\mathsf{A}}(\mathfrak{r}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{r})$. Wtedy:

$$\begin{aligned}
\mathsf{P}_{\mathsf{A}}(\mathfrak{s})\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{s})\mathsf{P}^{\mathsf{A}}(\mathfrak{t}) &= \\
\left(\mathsf{P}_{\mathsf{A}}(\mathfrak{r}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{r})\right)\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{r})\mathsf{P}^{\mathsf{A}}(\mathfrak{t}) &= \\
\mathsf{P}_{\mathsf{A}}(\mathfrak{r})\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{r})\left(\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}^{\mathsf{A}}(\mathfrak{t})\right) &= \\
\mathsf{P}_{\mathsf{A}}(\mathfrak{r})\mathsf{P}^{\mathsf{B}}(\mathsf{A} \star \mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{r})\mathsf{P}^{\mathsf{A}}(\mathsf{A} \star \mathfrak{t})
\end{aligned}$$

$\square$

Twierdzenie 3.3. Każda liczba pierwsza $p = 4k + 1$ jest sumą dwóch kwadratów liczb naturalnych.

Dowód. Z faktu 3.1 istnieje $4k$ słów o $p - 1$ podciągach. Pogrupujmy je w zbiory postaci $\{\mathfrak{s}, \mathfrak{s}^*, \bar{\mathfrak{s}}, \widetilde{\mathfrak{s}}\}$. Dla dowolnego słowa mamy $\mathfrak{s} \neq \mathfrak{s}^*$, więc każdy z tych zbiorów ma co najmniej dwa elementy – i będą to dwa elementy wtedy i

[3] Prawdę mówiąc, nie użyjemy jej bezpośrednio, ale będzie nam wskazywała drogę dowodu.

tylko wtedy gdy $\mathfrak{s} = \overline{\mathfrak{s}}$ lub $\mathfrak{s} = \widetilde{\mathfrak{s}}$, w przeciwnym zaś wypadku cztery. Wiemy już (Fakt 3.2), że mamy tylko dwa palindromy tworzące jedną grupę (będą to A^{p-2} oraz B^{p-2}), a ponieważ $p-1$ jest podzielne przez 4, to musimy mieć jeszcze jedną parę. Stąd w naszym zbiorze znajdziemy antypalindrom $\mathfrak{s}$ o $p-1$ podciągach.

Z Faktu 3.4 możemy zapisać $\mathfrak{s} = \mathfrak{t} \star \widetilde{\mathfrak{t}}$. Z Twierdzenia 3.2 otrzymujemy

$$p = \mathsf{P}(\mathfrak{s}) + 1 = \mathsf{P}_{\mathsf{A}}(\mathfrak{t})\mathsf{P}^{\mathsf{B}}(\widetilde{\mathfrak{t}}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{t})\mathsf{P}^{\mathsf{A}}(\widetilde{\mathfrak{t}}) = \mathsf{P}_{\mathsf{A}}(\mathfrak{t})^2 + \mathsf{P}_{\mathsf{B}}(\mathfrak{t})^2,$$

co kończy dowód. □

4 Poszukiwanie krótkich słów

Ja zaś zapytywałem siebie o teraźniejszość: jak jest szeroka i głęboka i ile z niej należy do mnie.

„Rzeźnia nr 5”
Kurt Vonnegut

W tym rozdziale powrócimy do pytania o możliwie krótkie słowa o danej liczbie podciągów. Zaczniemy od pytania prostszego, choć powiązanego – ile najwięcej podciągów można dostać dla słowa o danej długości.

Zdefiniujmy $\mathfrak{z}_0 = \mathsf{0}$, $\mathfrak{z}_{n+1} = \mathsf{A} \star \mathfrak{z}_n^*$ – to znaczy $\mathfrak{z}_n$ jest słowem składającym się na przemian z n liter A i B (zaczynając od tej pierwszej).

Twierdzenie 4.1. Jeśli $\mathfrak{s}$ jest słowem kończącym się na B (bądź pustym), to

$$\max_{|\mathfrak{t}|=n} \mathsf{P}(\mathfrak{s} \star \mathfrak{t}) = \mathsf{P}(\mathfrak{s} \star \mathfrak{z}_n)$$

Dowód. Będziemy dowodzić indukcyjnie po n. Dla $n = 0$ siłą rzeczy teza jest prawdziwa.

Niech $\mathfrak{t}$ będzie słowem dla którego to maksimum jest osiągnięte. Jeśli zaczyna się ono od A, to teza wynika z twierdzenia dla $(\mathfrak{s} \star \mathsf{A})^*$ i $n-1$. Jeśli zaś zaczyna się ono od B, to stosując twierdzenie dla $\mathfrak{s} \star \mathsf{B}$ i $n-1$ okaże się że możemy zastąpić $\mathfrak{t}$ przez $\mathfrak{z}_n^*$. Pozostaje więc udowodnić, że $\mathsf{P}(\mathfrak{s} \star \mathfrak{z}_n) \geqslant \mathsf{P}(\mathfrak{s} \star \mathfrak{z}_n^*)$, przy czym równość zachodzi tylko gdy $\mathfrak{s} = \mathsf{0}$.

Z Twierdzenia 3.2 wiemy, że $\mathsf{P}(\mathfrak{s} \star \mathfrak{t}) + 1 = \mathsf{P}_{\mathsf{A}}(\mathfrak{s})\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{s})\mathsf{P}^{\mathsf{A}}(\mathfrak{t})$. Wiemy, że $\mathsf{P}^{\mathsf{A}}(\mathfrak{z}_n) = \mathsf{P}^{\mathsf{B}}(\mathfrak{z}_n^*)$ oraz $\mathsf{P}^{\mathsf{B}}(\mathfrak{z}_n) = \mathsf{P}^{\mathsf{A}}(\mathfrak{z}_n^*)$. Skoro $\mathfrak{s}$ kończy się na B, to $\mathsf{P}_{\mathsf{B}}(\mathfrak{s}) \geqslant \mathsf{P}_{\mathsf{A}}(\mathfrak{s})$, przy czym równość zajdzie tylko gdy $\mathfrak{s}$ jest pusty. Ponadto $\mathsf{P}^{\mathsf{A}}(\mathfrak{z}_n) > \mathsf{P}^{\mathsf{B}}(\mathfrak{z}_n)$, zatem z twierdzenia o ciągach jednomonotonicznych po uwzględnieniu wcześniejszych równości dostajemy $\mathsf{P}(\mathfrak{s} \star \mathfrak{z}_n) \geqslant \mathsf{P}(\mathfrak{s} \star \mathfrak{z}_n^*)$, z równością tylko dla pustego $\mathfrak{s}$, co chcieliśmy właśnie udowodnić. □

Fakt 4.1. Spośród wszystkich słów długości n, $\mathfrak{z}_n$ oraz $\mathfrak{z}_n^*$ mają najwięcej, a konkretnie $F_{n+3} - 1$, podciągów.

Dowód. Pierwsza część to natychmiastowy wniosek z Twierdzenia 4.1. Co do drugiej, jasne że $\mathsf{P}(\mathfrak{z}_n) = \mathsf{P}(\mathfrak{z}_n^*)$. Zauważmy, że każdy podciąg $\mathfrak{z}_n$ można zapisać jako zaczynający się od jego pierwszej (tzn. A) lub drugiej (tzn. B) litery. W ten sposób

$$\mathsf{P}(\mathfrak{z}_n) + 1 = (\mathsf{P}(\mathfrak{z}_{n-1}) + 1) + (\mathsf{P}(\mathfrak{z}_{n-2}) + 1)$$

(pamiętamy o podciągu pustym), zatem z prostej indukcji dostajemy tezę. □

Ponieważ ze wzoru Bineta wiemy, że $F_n = \frac{1}{\sqrt{5}}\phi^n + o(1)$, w Faktu 4.1 wnioskujemy, że słowo długości n ma $O(\phi^n)$ podciągów. To w szczególności znaczy, że najkrótsze słowo o N podciągach ma długość $\Omega(\log N)$. Ten rezultat łatwo uogólnić na słowa o dowolnej liczbie liter – słowo o n literach ma 2^n podciągów (każdy znak możemy wziąć lub nie), więc także nie więcej niż 2^n różnych podciągów, i asymptotyka $\log N$ nadal działa (choć z gorszą stałą).

Nie jest zbyt trudno udowodnić szacowanie górne przez $O(\sqrt{N})$:

Fakt 4.2. Istnieje słowo o $N-1$ podciągach długości mniejszej niż $5\sqrt{2N}$.

Dowód. Szukamy takiego $a \in \left(\sqrt{\frac{1}{2}N}, \sqrt{8N}\right]$, że $\mathrm{nwd}(a, N) = 1$. Wtedy $\mathrm{gen}(N-a, a)$ będzie składał się z $\left\lfloor \frac{N-a}{a} \right\rfloor$ liter A złączonych ze słowem $\mathrm{gen}\left((N-a) \pmod a, a\right)$. Część pierwsza ma mniej niż $\frac{N}{a} < \sqrt{2N}$ liter, część druga zaś mniej niż $2a \leqslant 4\sqrt{2N}$ (w ogólności $|\mathrm{gen}(a,b)| < a+b$, gdyż podczas algorytmu Euklidesa suma obu liczb zmniejsza się w każdym kroku). Pozostaje znaleźć żądane a. Z twierdzenia Czebyszewa znajdziemy liczby pierwsze $p \in \left(\sqrt{\frac{1}{2}N}, \sqrt{2N}\right]$ oraz $q \in (\sqrt{2N}, \sqrt{8N}]$. Któraś z nich musi być względnie pierwsza z N – w przeciwnym razie dostalibyśmy $pq \mid N$, jednak $pq > N$, co dałoby sprzeczność. □

Jakkolwiek nie udało mi się osiągnąć lepszego wyniku, możemy próbować sformalizować intuicję, która sugerowała nam brać w rozwiązaniu zadania z Olimpiady $a \approx \frac{N+1}{\phi}$ – czyli jak dobrać takie liczby startowe, by serie kolejnych liter tego samego rodzaju nie były zbyt długie.

Dobierzmy zatem jakieś a, b względnie pierwsze i zastanówmy się, co dzieje się z ich ilorazem $\theta = \frac{a}{b}$ podczas wykonywania algorytmu Euklidesa. Jeśli $a > b$, widzimy że będzie to zmiana $\theta \to \theta - 1$. W przeciwnym zaś razie możemy zamienić liczby a i b, co odpowiada zmianie $\theta \to \theta^{-1}$, a następnie odjąć jeden. Ostatecznie algorytm kończy się, gdy $\theta = 1$.

Możemy zauważyć, że ten proces odpowiada rozwijaniu θ w ułamek łańcuchowy – to znaczy, że jeśli $\theta = [c_0; c_1, c_2, \ldots, c_k]$, to $\mathrm{gen}(a, b) = \mathsf{A}^{c_0}\mathsf{B}^{c_1}\mathsf{A}^{c_2}\ldots$ (na początku odejmujemy jedynkę c_0 razy, odwracamy ułamek, odejmujemy jedynkę c_1 razy, i tak dalej). Jeśli udałoby się, by wszystkie c_i były ograniczone przez C, to jako iż $\mathfrak{z}_{k+1}$ jest podciągiem $\mathrm{gen}(a, b)$ (zakładając bez straty ogólności $a > b$, czyli $c_0 \neq 0$), wiemy że $N = \mathsf{P}(\mathrm{gen}(a, b)) \geqslant \mathsf{P}(\mathfrak{z}_{k+1}) = F_{k+4} - 1$, więc $k = O(\log N)$, zatem $|\,\mathrm{gen}(a, b)| = \sum c_i = O(C \log N)$.

Niestety, jedna taka θ określa nam tylko jedno N, my zaś chcemy znaleźć krótkie słowo dla dowolnego N. Zastąpimy więc θ liczbą niewymierną o z góry zadanym rozwinięciu w ułamek łańcuchowy, i będziemy próbowali dobrać a tak, by $\frac{a}{M-a} \approx \theta$ (gdzie, jak wcześniej $M = N+1 = a+b$). Weźmy $x = \frac{M\theta}{\theta+1}$ i $y = \frac{M}{\theta+1}$, wtedy $\frac{x}{y} = \theta$ oraz $x + y = M$. Wybierzmy $a \approx x$ całkowite oraz $b = M - a$, niech $|a - x| = |b - y| = \varepsilon$. Intuicyjnie, algorytm Euklidesa dla pary (a, b) będzie przebiegał mniej więcej tak samo jak dla (x, y) – ponieważ będzie zachodzić $a > b \iff x > y$. Ta podwójna implikacja będzie prawdą dopóki suma błędów szacowania a przez x oraz b przez y nie wzrośnie powyżej $|x - y|$. Ponieważ ta druga wielkość będzie liniowo zależna od x ($\frac{x}{y}$ będzie zawsze liczbą niewymierną o ograniczonych mianownikach w ułamku łańcuchowym; takie zaś występują w pewnej, zależnej od tego ograniczenia lecz dodatniej, odległości od jedynki[4]), chcemy oszacować przede wszystkim jak szybko będzie rósł błąd.

Błąd we wszystkich momentach będzie wielokrotnością ε. Zauważmy, że jeśli odejmujemy liczby, błędy się dodają. To oznacza, że wykonując algorytm Euklidesa na $(a, b) = (x \pm \varepsilon, y \mp \varepsilon)$, jest on wykonywany w odwrotny sposób na współczynnikach przy ε. Jeśli w pewnym momencie przerwiemy wykonywanie algorytmu w momencie gdy posiadamy pewne słowo $\mathfrak{s}$, to sumaryczny błąd będzie równy $\mathsf{P}(\mathfrak{s})\varepsilon$. Jednocześnie, jeśli w tym czasie para (x, y) zmieni się w (z, w), to odwracając ten proces wychodząc od $(\max(w, z), \max(w, z))$ dostaniemy parę o sumie $\mathsf{P}(\mathfrak{s}) \cdot \max(z, w)$[5] – stąd $\max(z, w) \geqslant \frac{x+y}{\mathsf{P}(\mathfrak{s})}$. Ponieważ

[4] Tutaj będziemy przyjmować, że wartość C jest ustalona i niewielka. Podane tu metody mogą być zaadaptowane dla dowolnego C, jednak to wymaga uważniejszego przyjrzenia się asymptotyce.

[5] Tu korzystamy z faktu, iż $\mathsf{P}(\mathfrak{s}) = \mathsf{P}(\overline{\mathfrak{s}})$.

$\frac{x}{y}$ oraz $\frac{z}{w}$ będą ograniczone z dołu (jako liczby niewymierne o ograniczonym rozwinięciu w ułamek łańcuchowy), widać stąd że $z = O(\frac{x}{\mathsf{P(s)}})$, a to znaczy, że iloczyn $x \cdot \varepsilon$ wraz z czasem trwania algorytmu będzie utrzymywał się w pewnym stałym przedziale. Niech T będzie początkową wartością tego iloczynu. Ponieważ algorytm możemy wykonywać tak długo jak ε ma mniejszy rząd wielkości niż x, sytuacja ustabilizuje się gdy oba będą $O(\sqrt{T})$, co nastąpi po logarytmicznej względem N liczbie kroków (z argumentu jak wcześniej). W takim momencie przestajemy mieć kontrolę nad dalszą sekwencją odejmowań, i wiemy jedynie że będzie ona krótsza niż suma dwóch liczb które w tym momencie posiadamy, czyli $O(\sqrt{T})$. Zatem ostatecznie nasza długość słowa to $O(\log N + \sqrt{T})$, zaś ponieważ $x = O(N)$, jest to $O(\log N + \sqrt{\varepsilon N})$ – musimy więc zminimalizować ε.

Dodatkowym problemem jest warunek $\mathrm{nwd}(a, b) = 1$, który trudno uwzględnić z aproksymacyjnego punktu widzenia. Gdyby nie on, wzięcie dowolnego θ dałoby $\varepsilon = O(1)$ i długość słowa $O(\sqrt{N})$, która może nie jest wybitna, ale jest najlepszym rezultatem jaki osiągnęliśmy. Powtórzenie tego wraz z tym warunkiem wymaga szacowania, jak blisko x znajdziemy a względnie pierwsze z M; jeden z najlepszych wyników w tej kwestii zawarty jest w [2], za jego pomocą można pokazać istnienie $\varepsilon = O((\log M)^2)$, co przełoży się na słowo długości $O(\sqrt{N} \log N)$.

Można więc zastanowić się nad doborem odpowiedniego θ do N. Oczywiście dobór $\frac{a}{b} \approx \theta$ jest równoważny $\frac{b}{M} \approx \frac{1}{\theta+1}$, więc tak naprawdę chcemy aproksymować inną liczbę wymierną przez ułamek o mianowniku M, ponadto $|\frac{b}{M} - \frac{1}{\theta+1}| = \frac{1}{M}|b - y| = \frac{\varepsilon}{M}$, więc jeśli błąd takiej aproksymacji będzie równy δ, to długością słowa będzie $O(\log N + \sqrt{\delta N^2})$.

Twierdzenie Hurwitza mówi, że jeśli N będzie odpowiednie, δ rzeczywiście może być rzędu $\frac{1}{N^2}$, co da oczywiście logarytmiczną długość słowa. Do tego celu jednak N musi być mianownikiem w przybliżeniu θ otrzymanym z jej ułamka łańcuchowego. Okazuje się, że dla takich θ które dobraliśmy, czyli z ograniczonymi mianownikami w ułamku łańcuchowym, lepszego przybliżenia osiągnąć się nie da – istotnie, powyższy dowód można zaadaptować by to pokazać, gdyż T nie może być mniejsze od 1, bo skutkowałoby to tym, że algorytm musiałby trwać gdy $a = 0$ lub $b = 0$ (gdyż będą mniejsze od 1).

Ten optymistyczny przypadek, gdy N jest po prostu mianownikiem częściowego rozwinięcia θ, wedle hipotezy Zaremby uda się wygenerować zawsze, dla dostatecznie dużego C. Bourgain i Kontorovich udowodnili w [4], że hipoteza Zaremby (przy $C = 50$) jest prawdziwa dla N tworzących zbiór gęstości 1. Ich rezultat implikuje następujące:

Twierdzenie 4.2. Zbiór wszystkich N, dla których istnieje słowo długości co najwyżej $51 \log N$, o N podciągach, ma gęstość 1 w zbiorze liczb naturalnych.

W przypadku ogólnego N nie udało mi się jednak dokonać zadowalającego postępu. Chcielibyśmy oszacować odległość zbioru $S_C := \{[c_1, c_2, \ldots] \mid \forall i \; c_i \leqslant C\}$ od zbioru ułamków o mianowniku N, jednak skomplikowana topologia zbioru S_C (podobna do zbioru Cantora[6]) to utrudnia. Być może dokładniejsze opisanie struktury S_C da jakiś rezultat, do tego celu wydaje mi się jednak, że chcielibyśmy brać C rzędu większego niż stałe (co przy okazji psułoby nasze poprzednie szacowanie).

5 Iteracje i system Zeckendorfa

Rzeczywistość jest zawsze
bogatsza od naiwnych iluzji i
kłamliwych fikcji.

„Ferdydurke"
Witold Gombrowicz

Kuszące jest zinterpretowanie liczby jako słowa, to jest ciągu cyfr. W ten sposób nasze P można by rozważać jako funkcję z $\mathbb{N} \to \mathbb{N}$. Oczywiście wartości tej funkcji będą się zmieniały w zależności od tego jaki sposób zapisu liczb wybierzemy. Można wtedy rozważać funkcję P jako układ dyskretny, czyli patrzeć na zachowanie ciągów postaci $n,\ \mathsf{P}(n),\ \mathsf{P}^2(n), \ldots$ – ciągi takie będziemy nazywali *trajektoriami* dla n. Czy wychodząc od dowolnej liczby otrzymamy nieskończenie wiele innych wyrazów, czy może wpadniemy w cykl? Czy będziemy mieli jakieś punkty stałe? W przypadku klasycznych systemów pozycyjnych odpowiedź okazuje się nieskomplikowana i jest opisywana przez twierdzenie, które zaraz sformułujemy. Zauważmy jeszcze najpierw, że każda trajektoria jest zakończona jakimś cyklem, albo rozbiega do nieskończoności – istotnie, jeśli nie zachodzi druga opcja, to jej wyrazy są ograniczone, więc z zasady szufladkowej Dirichleta odwiedzimy pewien punkt dwa razy, więc od pewnego momentu trajektoria przebiega już zawsze trasę między dwoma wystąpieniami tego punktu (która tworzy cykl).

Twierdzenie 5.1. W zależności od podstawy systemu b zachowanie układu jest następujące:

- Dla $b \geqslant 5$ liczba 2 jest jedynym punktem stałym P, i jest jednocześnie atraktorem.

[6] W istocie, z twierdzenia Brouwera [5] wszystkie te zbiory będą homeomorficzne ze zbiorem Cantora.

- Dla $b = 4$ jedynymi punktami okresowymi (a nawet stałymi) są 2 i 4.
- Dla $b = 3$ jedyne cykle to (2) i $(3, 4)$, przy czym wszystkie trajektorie startujące od $x \geqslant 3$ wpadają w drugi z nich.
- Dla $b = 2$ cyklami są (3), (6), (8), (18) oraz $(9, 11, 10, 12)$.

We wszystkich przypadkach nie ma trajektorii rozbiegających do nieskończoności (w szczególności wszystkie kończą się w jakimś z dostępnych cykli).

Dowód. Przyjmijmy, że liczba x spełnia $b^{n-1} \leqslant x < b^n$ – wtedy x ma n znaków w zapisie o podstawie b, zatem $\mathsf{P}(x) \leqslant 2^n$. Jeśli $2^n < b^{n-1}$, to $\mathsf{P}(x)$ będzie miało mniej znaków niż x, i ta tendencja będzie się utrzymywać dopóki nierówność zachodzi. Dla $b \geqslant 5$ wystarczy $n \geqslant 2$ – więc wszystkie trajektorie napotkają element jednoznakowy, który ma dwa podciągi – 2 jest więc atraktorem i jednocześnie punktem stałym.

Dla $b \in \{3, 4\}$ potrzebujemy $n \geqslant 3$, czyli trajektorie zawsze osiągną liczbę dwucyfrową. Każda taka liczba ma najwyżej cztery podciągi, więc ostatecznie zawsze napotkamy liczbę nie większą niż cztery, i ręcznie możemy sprawdzić, że jedyne cykle dla nich to te w sformułowaniu twierdzenia. Dla $b = 3$ będziemy mieli $\mathsf{P}^{-1}(2) = \{1, 2\}$ i $\mathsf{P}^{-1}(1) = \varnothing$, więc cykl złożony z dwójki będzie nieosiągalny dla $x \geqslant 3$.

Pozostaje przypadek $b = 2$ dla którego nasze obecne szacowanie nie zachodzi nigdy. Wiemy natomiast, że liczby w systemie dwójkowym mają tylko dwie możliwe cyfry; jeśli więc $2^{n-1} \leqslant x < 2^n$, to z Faktu 4.1 mamy $\mathsf{P}(x) \leqslant F_{n+3} - 1$. Jeśli $F_{n+3} \leqslant 2^{n-1}$, to $\mathsf{P}(x)$ będzie miało mniej cyfr niż x. Ta nierówność zachodzi dla $n \geqslant 7$ (dla $n = 7$ mamy $64 > 55$, wyżej używamy prostej indukcji, jako iż $2F_m \geqslant F_{m+1} = F_m + F_{m-1}$), każda trajektoria osiąga więc wartość mniejszą od 64.

Podobna nierówność, $F_{n+3} \leqslant 2^n$, zachodzi od $n = 3$ – w tych przypadkach oznacza ona, że $\mathsf{P}(x)$ ma co najwyżej tyle samo cyfr ile x. Jeśli x ma 6 cyfr, $\mathsf{P}(x) \leqslant 33 = F_{6+3} - 1$, więc $\mathsf{P}(x)$ należy do $\{32, 33\}$ lub ma co najwyżej pięć cyfr. W obydwu tych przypadkach $\mathsf{P}(\mathsf{P}(x))$ ma nie więcej niż 5 cyfr (co sprawdzamy po policzeniu $\mathsf{P}(32) = 12$ oraz $\mathsf{P}(33) = 19$). Analogicznie gdy x ma pięć cyfr, $\mathsf{P}(x)$ będzie miało co najwyżej cztery cyfry, lub będzie w przedziale $[16, 20]$. Przypadek $x = 18$ da punkt stały, pozostałe przypadki ($20 \to 17 \to 15$ oraz $19 \to 16 \to 10$) zakończą się na liczbach czterocyfrowych. I znowu – dla x o co najwyżej czterech cyfrach, $\mathsf{P}(x) \leqslant 12$, więc albo dana trajektoria wpada w punkt stały równy 18, albo kończy się w przedziale $[1, 12]$ (i go nie opuszcza). Zostało nam dwanaście przypadków do sprawdzenia, wystarczy więc sprawdzić istnienie pozostałych czterech cykli umieszczonych w treści twierdzenia, oraz trajektorie $1 \to 2 \to 4 \to 6$ i $5 \to 7 \to 6$ obejmujących pięć pozostałych przypadków. □

Przykład. W przypadku systemu dwójkowego przykładowa trajektoria to $39 \to 21 \to 20 \to 17 \to 15 \to 5 \to 7 \to 4 \to 6 \to 6 \to \dots$

Widzimy, że we znaki daje się różna asymptotyka funkcji P i systemów pozycyjnych. W dalszej części będziemy przez cały czas rozważali *system Zeckendorfa*, w którym liczba o n cyfrach będzie rzędu F_n.

Definicja 5.1. W systemie Zeckendorfa cyframi są 0 i 1, przy czym w zapisie żadnej liczby nie możemy użyć dwóch jedynek z rzędu. Cyfra stojąca na i-tej pozycji od prawej (licząc od zera) ma wartość F_{i+2}.

Dowód, że system Zeckendorfa jest poprawnie zdefiniowany, można znaleźć na przykład w [1].

Przykład. Kolejne liczby zapisane w systemie Zeckendorfa to $1,\ 10,\ 100,\ 101,\ 1000, \dots$. Liczbę 100 zapisujemy jako sumę liczb Fibonacciego $89+8+3$, co odpowiada zapisowi 1000010100.

Fakt 5.1. $\mathsf{P}(F_k - 1) = \mathsf{P}(F_{k+1} - 1)$

Zanim przejdziemy do dowodu, chciałbym podkreślić, że aby uniknąć w przyszłości konfuzji, utożsamimy cyfrę 1 z literą A oraz cyfrę 0 z literą B, i będziemy stosować te notacje zamiennie, skłaniając się ku literowej jeśli użycie cyfr mogłoby być mylące.

Dowód. Zapis liczby $F_k - 1$ jest największym odpowiadającym liczbie mniejszej niż F_k, będzie miał więc $k-2$ cyfry i będzie składał się z cyfr 1 i 0 na przemian. Jednym słowem, będzie on równy $\mathfrak{z}_{n-2}$ (modulo zmiana alfabetu o której pisaliśmy wcześniej), będzie miał więc $F_{n+1} - 1$ podciągów. □

Zatem tutaj, w przeciwieństwie do wcześniejszych systemów, mamy trajektorię uciekającą do nieskończoności. Ta rozbieżność jednak jest ograniczona: liczba k-cyfrowa ma wartość $\geqslant F_{k+1}$ i mniej niż F_{k+3} podciągów, więc $\limsup \frac{\mathsf{P}(x)}{x} \leqslant \phi^2$. W dalszej części rozdziału pokażemy, że $\mathsf{P}(x) < 1.7237x$ dla dużych x.

O ile trajektoria wychodząca od jedynki będzie, jak pokazaliśmy, nieograniczenie rosnąć, to ustawiając punkt startowy na przykład na liczbie 3, okaże się, że po szesnastu krokach otrzymamy 112, które jest punktem stałym. Za pomocą obliczeń komputerowych możemy znaleźć inne punkty stałe, takie jak $36,\ 78,\ 887,\ 8314$ oraz 4656039, a także cykle $(39, 42)$, $(52, 59, 60)$, $(743, 925, 1147)$ oraz $(27, 44, 70, 91, 48, 50, 66, 90, 35)$ – są to wszystkie ich przykłady do 10^7. Na tej dziesięciomilionowej próbce okazuje się[7], że trajektorie około 30% punktów początkowych kończą się w 112, 29% w $(52, 59, 60)$, 21% w naszym ciągu Fibonacciego minus jeden, zaś 11% w 9-cyklu zaczynającym się od 27.

Można przypuszczać, że takich cykli, a nawet punktów stałych, znajdziemy nieskończenie wiele, a ich zachowanie jest dosyć nieregularne. W dalszej części pracy scharakteryzujemy ogólną strukturę zapisu Zeckendorfa punktów stałych, jednak będzie to dalekie od ich pełnego opisu.

Wprowadzimy teraz bardzo istotną koncepcję, dzięki której będziemy mogli skuteczniej badać liczby podciągów oraz punkty stałe P.

Definicja 5.2. Słowo $\mathfrak{s}$ utożsamimy z macierzą

$$M(\mathfrak{s}) = \begin{pmatrix} \mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s}) & \mathsf{P}_{\mathsf{B}}^{\mathsf{B}}(\mathfrak{s}) \\ \mathsf{P}_{\mathsf{A}}^{\mathsf{A}}(\mathfrak{s}) & \mathsf{P}_{\mathsf{B}}^{\mathsf{A}}(\mathfrak{s}) \end{pmatrix}$$

Przykład. Możemy policzyć, że $M(\mathsf{ABA}) = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$. Można także zauważyć, skąd nasze dziwne reguły uwzględniania podciągu pustego – przy naszej konwencji zachodzi naturalna równość $M(\mathsf{0}) = I$.

Lemat 5.1. Jeśli $\mathfrak{r}$ jest słowem powstałym z $\mathfrak{s}$ przez odcięcie fragmentu do pierwszej litery B (z nią włącznie), to:

- $\mathsf{P}^{\mathsf{B}}(\mathfrak{s}) = \mathsf{P}(\mathfrak{r}) + 1$
- $\mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s}) = \mathsf{P}_{\mathsf{A}}(\mathfrak{r})$
- $\mathsf{P}_{\mathsf{B}}^{\mathsf{B}}(\mathfrak{s}) = \mathsf{P}_{\mathsf{B}}(\mathfrak{r})$

Dowód. Zauważmy, że podciągi $\mathfrak{s}$ rozpoczynające się na B to $\mathsf{0}$ oraz podciągi niepuste. Te drugie możemy zapisać jako konkatenację pierwszej litery B w $\mathfrak{s}$ z jakimś podciągiem $\mathfrak{r}$, stąd żądana równość.

Analogiczna uwaga działa dla drugiego podpunktu, z tą różnicą, że teraz po obu stronach mamy podciągi puste, które nie przechodzą na nic w takich bijekcjach. W trzecim podpunkcie znów mamy podobnie, ale „niesparowanymi” podciągami są B po lewej stronie (nie wliczamy tu pustego) oraz pusty po prawej, zatem znowu zachodzi równość. □

[7] Podział ten zdaje się zachowywać dosyć stabilnie wraz ze wzrostem zakresu, który testujemy (wyniki już dla 10^4 będą bardzo podobne), z drugiej strony skala dostępna dla komputera nie da istotnych z matematycznego punktu widzenia wyników, tak więc nie przypuszczam by na przykład istniały granice tych ułamków.

Twierdzenie 5.2. Odwzorowanie M jest homomorfizmem (monoidów) z $\mathcal{M}_2 \to \mathrm{SL}_2(\mathbb{Z})$.

Dowód. Musimy udowodnić, że $M(\mathfrak{s} \star \mathfrak{t}) = M(\mathfrak{s})M(\mathfrak{t})$ oraz że $\det M(\mathfrak{s}) = 1$. Pierwsza z tych równości składa się tak naprawdę z czterech, dla każdego współczynnika z osobna, na przykład:

$$\mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s} \star \mathfrak{t}) = \mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s})\mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}^{\mathsf{B}}(\mathfrak{s})\mathsf{P}_{\mathsf{A}}^{\mathsf{A}}(\mathfrak{t})$$

Ponieważ wszędzie interesują nas tylko podciągi zaczynające się od B i kończące na A, to możemy odciąć fragment $\mathfrak{s}$ do pierwszego B oraz fragment $\mathfrak{t}$ od ostatniego A, dostając (z Lematu 5.1) do udowodnienia dla pozostałych części tych słów równość

$$\mathsf{P}(\mathfrak{s} \star \mathfrak{t}) + 1 = \mathsf{P}_{\mathsf{A}}(\mathfrak{s})\mathsf{P}^{\mathsf{B}}(\mathfrak{t}) + \mathsf{P}_{\mathsf{B}}(\mathfrak{s})\mathsf{P}^{\mathsf{A}}(\mathfrak{t}),$$

która wynika z Twierdzenia 3.2.

Aby udowodnić drugą część, zauważmy, że

$$M(\mathsf{A}) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

oraz $M(\mathsf{B}) = M(\mathsf{A})^T$, więc $\det M(\mathsf{A}) = \det M(\mathsf{B}) = 1$. Ponieważ wyznacznik jest multiplikatywny, a M, jak udowodniliśmy, jest homomorfizmem, to macierz odpowiadająca każdemu słowu będzie miała wyznacznik 1, co właśnie chcieliśmy udowodnić.

□

Stąd dostajemy natychmiastowy wniosek

Fakt 5.2.

$$\mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s})\mathsf{P}_{\mathsf{B}}^{\mathsf{A}}(\mathfrak{s}) = \mathsf{P}_{\mathsf{A}}^{\mathsf{A}}(\mathfrak{s})\mathsf{P}_{\mathsf{B}}^{\mathsf{B}}(\mathfrak{s}) + 1$$

Będziemy oznaczali skrótowo $A = M(\mathsf{A})$, $B = M(\mathsf{B})$. Gdy zastanowimy się, jakie wartości liczby poszczególnych podciągów mogą przyjmować modulo jakieś q, okaże się, że powyższa równość jest jedynym ograniczeniem.

Twierdzenie 5.3. Dla dowolnego $q = \mathbb{N}$ oraz $k,\ l,\ m,\ n \in \mathbb{Z}$ takich, że $kn - lm \equiv 1 \pmod{q}$, istnieje $\mathfrak{s} \in \mathcal{M}_2$ takie, że

- $k \equiv \mathsf{P}_{\mathsf{A}}^{\mathsf{B}}(\mathfrak{s}) \pmod{q}$
- $l \equiv \mathsf{P}_{\mathsf{A}}^{\mathsf{A}}(\mathfrak{s}) \pmod{q}$
- $m \equiv \mathsf{P}_{\mathsf{B}}^{\mathsf{B}}(\mathfrak{s}) \pmod{q}$

- $n \equiv \mathsf{P}^{\mathsf{A}}_{\mathsf{B}}(\mathfrak{s}) \pmod q$

Dowód. Oczywiście z Twierdzenia 5.2 wystarczy pokazać, że A i B generują całe $\mathrm{SL}_2(\mathbb{Z}_q)$ jako monoid. Jednak możemy zauważyć indukcyjnie, że

$$A^t = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix},$$

w szczególności $A^{q-1} \equiv A^{-1} \pmod q$ – zatem wystarczy, że będzie to generowanie jako grupa. Ponieważ można udowodnić (na przykład [3]), że generatorami $\mathrm{SL}_2(\mathbb{Z})$ są B oraz $AB^{-1}A$, zostaje pokazać, że operacja brania macierzy modulo q jest surjektywnym odwzorowaniem z $\mathrm{SL}_2(\mathbb{Z})$ na $\mathrm{SL}_2(\mathbb{Z}_q)$, czyli że pewna macierz z $\mathrm{SL}_2(\mathbb{Z})$ przystaje do $\begin{pmatrix} k & l \\ m & n \end{pmatrix}$ modulo q.

Skoro $kn - ml \equiv 1 \pmod q$, to $\mathrm{nwd}(k, l, q) = 1$. Zauważmy, że zmiana $m \to m + q$ odejmuje od wyznacznika lq, zaś $n \to n + q$ dodaje kq. Jeśli mielibyśmy $\mathrm{nwd}(k, l) = 1$, to z tożsamości Bezout tymi transformacjami moglibyśmy ustalić wyznacznik na dowolnej liczbie $\equiv kn - ml \pmod q$, w szczególności jedynce. Zostaje więc dokonać takiej zmiany l, by faktycznie było względnie pierwsze z k, czyli znaleźć takie a, że $\mathrm{nwd}(k, l + aq) = 1$. Dla każdego dzielnika pierwszego $p \mid k$, mamy albo $p \mid q$, więc $p \nmid l$ i $p \nmid l + aq$ w żadnym przypadku, albo $p \nmid q$, i warunek $p \mid l + aq$ możemy przepisać na jedną kongruencję postaci $a \not\equiv c \pmod p$. Z chińskiego twierdzenia o resztach znajdziemy takie a, że wszystkie te warunki będą jednocześnie zachodzić, więc $\mathrm{nwd}(k, l + aq) = 1$ co kończy dowód. $\square$

Jeśli oznaczymy $v = (1, 1)^T$, to z definicji $M(\mathfrak{s})$ natychmiastowo dostajemy

Fakt 5.3.
$$\mathsf{P}(\mathfrak{s}) = v^T M(\mathfrak{s}) v - 1$$

Oczywiście współczynniki macierzy $M(\mathfrak{s})$ są nieujemne. Możemy wprowadzić częściowy porządek na macierzach: $M_1 \leqslant M_2$, jeśli wszystkie współczynniki M_1 są mniejsze lub równe odpowiednim współczynnikom w M_2; łatwo wtedy zauważyć, że na macierzach o współczynnikach nieujemnych mnożenie będzie zachowywało ten porządek, tj. $M_1 \leqslant M_2$ implikuje $M_1 N \leqslant M_2 N$ oraz $N M_1 \leqslant N M_2$ (wystarczy odjąć te nierówności stronami i zauważyć, że iloczyn dwóch macierzy N oraz $M_2 - M_1$ o nieujemnych współczynnikach, także ma współczynniki nieujemne). Te same własności będą zachodzić dla N o dowolnych wymiarach (byle tylko mnożenie było dobrze zdefiniowane), w szczególności na przykład dla wektorów.

Lemat 5.2. $\mathsf{P}(\mathfrak{s}\star \mathsf{ABABA}\star \mathfrak{t}) \geqslant \frac{8}{5}\mathsf{P}(\mathfrak{s}\star \mathsf{AAAAA}\star \mathfrak{t})$

Dowód. Wiemy, że

$$M(\mathsf{ABABA}) = \begin{pmatrix} 5 & 3 \\ 8 & 5 \end{pmatrix},\ M(\mathsf{AAAAA}) = \begin{pmatrix} 1 & 0 \\ 5 & 1 \end{pmatrix},$$

więc $M(\mathsf{ABABA}) \geqslant \frac{8}{5}M(\mathsf{AAAAA})$. To oznacza także

$$v^T M(\mathfrak{s})M(\mathsf{ABABA})M(\mathfrak{t})v \geqslant \frac{8}{5}v^T M(\mathfrak{s})M(\mathsf{AAAAA})M(\mathfrak{t})v,$$

co po użyciu Faktu 5.3 (i odjęciu 1 od lewej, zaś $\frac{8}{5}$ od prawej, co tylko wzmocni nierówność) kończy dowód. □

To pozwala nam na pierwszy rezultat odnośnie dynamiki P.

Fakt 5.4. Jeśli n zawiera piętnaście zer z rzędu, to $\mathsf{P}(n) < n$.

Dowód. Rozważmy n w systemie Zeckendorfa, które ma m cyfr oraz spójny fragment 15 zer. Z poprzedniego lematu, zamieniając wszystkie piątki AAAAA na ABABA liczba podciągów wzrośnie co najmniej $\left(\frac{8}{5}\right)^3$ razy. Po tej zamianie otrzymamy słowo o m literach, które z Faktu 4.1 ma co najwyżej $F_{m+3} - 1$ podciągów. Zatem skoro $n \geqslant F_{m+1}$, to

$$\frac{\mathsf{P}(n)}{n} \leqslant \frac{\left(\frac{5}{8}\right)^3 (F_{m+3} - 1)}{F_{m+1}} \leqslant \left(\frac{5}{8}\right)^3 \phi^2 \approx 0.63917 < 1$$

(szacowanie $F_{k+3} - 1 \leqslant \phi^2 F_{k+1}$ wynika w prosty sposób ze wzoru Bineta). To kończy dowód.

□

Podobnymi metodami można dowodzić, że dla dowolnego $\varepsilon > 0$ zbiór takich n, że $\mathsf{P}(n) > \varepsilon n$, ma zerową gęstość w zbiorze liczb naturalnych. Później wzmocnimy Fakt 5.4 w faktach 5.5 i A.1.

Przyjmiemy na $\mathbb{R}^2$ normę $||(x,y)||_p = \sqrt[p]{|x|^p + |y|^p}$, oraz normę na macierzach rzeczywistych o wymiarach 2×2: $||M||_p = \sup_{v \neq (0,0)} \frac{||Mv||_p}{||v||_p}$.

Twierdzenie 5.4.

$$\mathsf{P}(\mathfrak{s}) \leqslant 2||M(\mathfrak{s})||_2 - 1$$

Dowód.

$$\begin{aligned} \mathsf{P}(\mathfrak{s}) = v^T M(\mathfrak{s})v - 1 = ||M(\mathfrak{s})v||_1 - 1 \leqslant \\ \leqslant \sqrt{2}||M(\mathfrak{s})v||_2 - 1 \leqslant \sqrt{2}||M(\mathfrak{s})||_2||v||_2 - 1 = 2||M(\mathfrak{s})||_2 - 1 \end{aligned}$$

przy czym pierwsza z tych nierówności wynika z nierówności między średnią kwadratową a arytmetyczną $||w||_1 \leqslant \sqrt{2}||w||_2$. $\square$

Zauważmy, że $||M(\mathfrak{s})||_2$ to największa wartość singularna $M(\mathfrak{s})$. Stąd $||A||_2 = \phi$, gdyż ϕ^2 jako pierwiastek $x^2 - 3x + 1$ jest największą wartością własną AA^T. Stąd faktycznie nasze szacowanie jest w jakiś sposób optymalne – każda nowa litera zwiększa je ϕ razy, czyli o tyle o ile może zwiększać się liczba podciągów. Dla dużych macierzy możemy użyć szacowania $||M||_2 \leqslant \sqrt{\operatorname{tr} MM^T}$, gdyż największa wartość własna MM^T (czyli kwadrat wartości singularnej M) jest pierwiastkiem $x^2 - \operatorname{tr}(MM^T)x + 1 = 0$, jest więc nieco mniejsza niż $\operatorname{tr} MM^T$.

Twierdzenie 5.4 pozwala nam, korzystając z submultiplikatywności normy, dowodzić pewne „strukturalne” twierdzenia o $\mathsf{P}(\cdot)$, takie jak na przykład

Fakt 5.5. Jeśli n zawiera sześć zer z rzędu, to $\mathsf{P}(n) < n$.

Dowód. Niech $F_{k+1} \leqslant n < F_{k+2}$, to znaczy n ma w zapisie k znaków. Wiemy, że $\operatorname{tr} B^6 A^6 = 38$, więc $\mathsf{P}(n) \leqslant 2||M(n)||_2 - 1 \leqslant 2\phi^{k-6}\sqrt{38} - 1$. Jednocześnie ze wzoru Bineta $n \geqslant F_{k+1} \geqslant \frac{1}{\sqrt{5}}\phi^{k+1} - 1$. Wystarczy więc udowodnić $\frac{1}{\sqrt{5}}\phi^{k+1} \geqslant 2\phi^{k-6}\sqrt{38}$, czyli

$$\phi^7 \approx 29.03444 \geqslant 2\sqrt{5} \cdot \sqrt{38} \approx 27.56810$$

$\square$

Zdefiniujemy *deficyt* słowa, $\delta(\mathfrak{s}) := \frac{||M(\mathfrak{s})||_2}{\phi^{|\mathfrak{s}|}}$. Fakt 5.5 jest szczególnym przypadkiem poniższego stwierdzenia:

Lemat 5.3. Jeśli $\delta(n) \leqslant \frac{\phi}{2\sqrt{5}} \approx 0.36180$, to $\mathsf{P}(n) < n$.

Dowód. Niech n ma k znaków, to znaczy $F_{k+2} > n \geqslant F_{k+1}$. Wiemy, że $\mathsf{P}(n) \leqslant 2||M(n)||_2 - 1 = 2\phi^k\delta(n) - 1 \leqslant \frac{\phi^{k+1}}{\sqrt{5}} - 1 < F_{k+1}$, co kończy dowód. $\square$

Jeśli oznaczymy $\psi(\mathfrak{s}) = -\ln \delta(\mathfrak{s})$, submultiplikatywność normy przeniesie się na własność $\psi(\mathfrak{s} \star \mathfrak{t}) \geqslant \psi(\mathfrak{s}) + \psi(\mathfrak{t})$ (przy czym ψ będzie przyjmowała wartości nieujemne, gdyż wartości δ leżą w $[0, 1]$). Ponadto ψ od pojedynczej litery będzie równe, oczywiście, zero. Jeśli więc znajdziemy takie rozłączne podsłowa w n, dla których suma ψ będzie przekraczać $-\ln(\frac{\phi}{2\sqrt{5}}) \approx 1.01665$, będziemy wiedzieli z lematu 5.3, że $\mathsf{P}(n) < n$ (na przykład w szczególności n nie może być punktem stałym P).

Naturalne rozłączne cząstki n są blokami postaci AB^k (być może $k = 0$, ale tylko jeśli jest to blok końcowy). Dobrym pomysłem więc zdaje się policzenie wartości ψ dla takich bloków[8]:

k	$\psi(\mathsf{AB}^k)$
0, 1	0
2	0.09185
3	0.27762
4	0.52573
5	0.81583
6	1.13559

Tabela 1: Wartości funkcji ψ.

Bloki postaci AB^k dla $k > 1$ będziemy nazywali ψ-dodatnimi. Stąd jeśli zapis punktu stałego n zawiera a bloków AB^2, b bloków AB^3, c bloków AB^4 oraz d bloków AB^5, to

$$0.09185a + 0.27762b + 0.52573c + 0.81583d < 1.01665$$

Nierówność ta ma 42 rozwiązania w $a,\ b,\ c,\ d \geqslant 0$, co jest wynikiem niemałym, acz skończonym. W dodatku A zredukujemy tę liczbę do dwudziestu.

Rozdział (a także „właściwą” część pracy) zakończymy dwoma twierdzeniami, które starają się opisać dokładnie jakie wartości może przyjąć $\mathsf{P}(n)$, oraz ile razy może być ono większe od n. Ich dowody przedstawimy jednak już w dodatku, tutaj tylko nakreślając ich początek i dalszą ideę postępowania.

Twierdzenie 5.5.

$$\limsup_{x\to\infty} \frac{\mathsf{P}(x)}{x} = \frac{2\phi + 3}{\phi + 2} \approx 1.72361$$

Zarys dowodu. Zaczniemy od pokazania, że dla pewnego ciągu x rzeczywiście osiągniemy tę granicę. Weźmy $x = F_{k+2} + F_k - 1$. Zapisem x w systemie Zeckendorfa jest $1001010\ldots$ z $k+1$ cyframi (po dodaniu jedynki musi być to 101 oraz $k-2$ zer). Możemy zapisać więc x jako $100\star\mathfrak{z}_{k-2}$. Z Twierdzenia 3 (oraz dowodu faktu 5) otrzymujemy

[8] Przy czym największą wartość singularną macierzy M możemy policzyć poprzez wzór $\sqrt{\frac{\operatorname{tr} MM^t + \sqrt{(\operatorname{tr} MM^T)^2 - 4}}{2}}$.

$$\mathsf{P} = \mathsf{P}_0(100)\mathsf{P}^1(\mathfrak{z}_{k-2}) + \mathsf{P}_1(100)\mathsf{P}^0(\mathfrak{z}_{k-2}) - 1 = 5F_k + 2F_{k-1} - 1,$$

więc, ponieważ $\frac{F_{k+1}}{F_k} \to \phi$

$$\frac{\mathsf{P}(x)}{x} = \frac{5F_k + 2F_{k-1} - 1}{F_{k+2} + F_k - 1} \to \frac{5\phi + 2}{\phi^3 + \phi} = \frac{2\phi^2 + 3\phi}{\phi^3 + \phi} = \frac{2\phi + 3}{\phi + 2},$$

(gdzie korzystamy kilkukrotnie z tego, że $\phi^2 = \phi + 1$).

Aby pokazać, że nie da się więcej, udowodnimy w przyszłości, że każdy taki potencjalny kandydat zaczyna się od 100. Jeśli nie będzie postaci takiej jak wyżej, to znajdziemy w niej jeszcze jeden blok o dodatnim ψ (albo po wiodącej jedynce znajdziemy więcej zer), co po dokładniejszym przeliczeniu pozwoli nam stwierdzić, że taka sytuacja jest niemożliwa.

Twierdzenie 5.6. Jeśli $m \neq 1, 3, 5, 9, 13, 21, 29, 45, 61$ oraz[9] $m \neq 2 \cdot 16^t - 3$, to istnieje n takie, że $\mathsf{P}(n) = m$.

Zarys dowodu. W naturalny sposób $2k = \mathsf{P}(\mathsf{AB}^{k-1})$ dla $k \geqslant 1$, więc musimy przejmować się tylko liczbami nieparzystymi. Będziemy chcieli policzyć $\mathsf{P}(\mathsf{AB}^k\mathsf{AB}^l)$. Zauważmy, że

$$AB^k = \begin{pmatrix} 1 & k \\ 1 & k+1 \end{pmatrix}$$

więc

$$1 + \mathsf{P}(\mathsf{AB}^k\mathsf{AB}^l) = v^T AB^k AB^l v = \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & k \\ 1 & k+1 \end{pmatrix} \begin{pmatrix} 1 & l \\ 1 & l+1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} =$$
$$= \begin{pmatrix} 2 & 2k+1 \end{pmatrix} \begin{pmatrix} l+1 \\ l+2 \end{pmatrix} = (2k+1)(l+2) + 2(l+1) =$$
$$= 2kl + 3l + 4k + 4 = (2k+3)(l+2) - 2$$

Ostatecznie więc (pamiętając o jedynce) chcemy, by $(2k+3)(l+2) = n+3$. Potrzebujemy $k \geqslant 1$, $l \geqslant 0$ (potrzebujemy odstępu między A), więc pierwszy z tych czynników może być dowolną liczbą nieparzystą $\geqslant 5$, drugi zaś dowolną liczbą naturalną większą od 1. Skoro n jest nieparzyste, to $n+3$ jest parzyste, więc tak czy tak sytuacja w której potrzebowalibyśmy $l+2 = 1$ jest niemożliwa – zatem chcemy by $n+3$ miało dzielnik nieparzysty większy od 3. Jedyne sytuacje w których tak nie jest, to $n = 2^t - 3$ lub $n = 3 \cdot 2^t - 3$, i część z nich da się wykluczyć przez rozpatrywanie słów złożonych z trzech bloków, co zrobimy w Dodatku.

[9] Warunek drugi prawdopodobnie nie jest wymagany, o czym napiszemy w dodatku B.

A Szczegóły, szczególiki

Ale kiedy dałem już za wygraną
i wróciłem na chodnik, upadło
przede mną na lśniący asfalt
parę kolorowych świetlnych liter.
Czytałem:
Tylko dla obłąkanych!

„Wilk stepowy”
Hermann Hesse

W tym dodatku będziemy dowodzili rezultatów, których dowody uznałem za zbyt obliczeniowe, aby weszły we „właściwą część” pracy. Czytelnikowi Nieufnemu, który zamierza na bieżąco sprawdzać wartości podawanych przez nas wyrażeń, polecamy zaopatrzyć się co najmniej w kalkulator naukowy, a najlepiej w system algebry komputerowej.

Zaczniemy od lematu, który pozwoli nam uwzględnić drugą stronę relacji między $\mathsf{P}(n)$ a n. Oznaczmy przez $\xi(n)$ liczbę, którą otrzymamy z zapisu Zeckendorfa n przez zastąpienie wag F_k liczbami $\frac{1}{\sqrt{5}}\phi^k$.

Lemat A.1. $|\xi(n) - n| \leqslant \frac{1}{\sqrt{5}}$

Dowód. Ze wzoru Bineta różnica F_k oraz $\frac{1}{\sqrt{5}}\phi^k$ to $\frac{1}{\sqrt{5}}(-\varphi)^k$. Ponieważ jedyne k dla jakich wykonujemy tę operację, to $k \geqslant 2$, sumaryczny błąd jaki popełnimy będzie nie większy od

$$\frac{1}{\sqrt{5}}\left(\varphi^2 + \varphi^3 + \varphi^4 + \ldots\right) = \frac{1}{\sqrt{5}}\frac{\varphi^2}{1-\varphi} = \frac{1}{\sqrt{5}}$$

□

Jeśli n ma k znaków, oznaczmy $\lambda(n) := \frac{\xi(n)\sqrt{5}}{\phi^{k+1}}$. Powyższy lemat ten pozwala nam wzmocnić lemat 5.3 do następującego twierdzenia:

Twierdzenie A.1. Jeśli dla pewnej stałej $\kappa \leqslant 2$ mamy

$$\delta(n) \leqslant \frac{\phi}{2\sqrt{5}}\lambda(n)\kappa,$$

to $\mathsf{P}(n) < \kappa n$.

Dowód. Postępujemy jak w dowodzie Lematu 5.3: niech n ma k znaków, wtedy $\mathsf{P}(n) \leqslant 2\phi^k\delta(n) - 1 \leqslant \frac{\phi^{k+1}}{\sqrt{5}}\lambda(n)\kappa - 1 = \xi(n)\kappa - 1$, wystarczy więc oszacować $(\xi(n) - n)\kappa < 1$, co wynika z Lematu A.1. □

Logarytmując obie strony nierówności z Twierdzenia A.1, dostajemy równoważne sformułowanie

$$\psi(n) + \ln(\lambda(n)) + \ln(\kappa) \geqslant \ln\left(\frac{\phi}{2\sqrt{5}}\right) \approx 1.01665$$

Wartość $\lambda(n)$ jest sumą ϕ^{-i} po takich i, że na i-tym miejscu od lewej zapisu n znajduje się jedynka (licząc miejsca od zera). W szczególności jeśli m jest prefiksem n, to $\lambda(m) \leqslant \lambda(n)$. To pozwala nam oszacować z dołu $\lambda(n)$ w zależności od prefiksu n.

k	$\ln(\lambda(\mathsf{AB}^k\mathsf{A}))$
1	0.32351
2	0.21194
3	0.13619
4	0.08633
5	0.05423

Tabela 2: Wartości funkcji λ.

Dalszy ciąg dowodu Twierdzenia 5.5. Biorąc $\kappa = \frac{2\phi+3}{\phi+2}$ powyżej, dostajemy $\ln(\kappa) \approx 0.54442$, zatem jakikolwiek kontrprzykład do naszego szacowania musi spełniać $\psi(n) + \ln(\lambda(n)) \leqslant 0.47223$. Patrząc na Tabelę 1, widzimy, że blok AB^4 ani żaden większy nie może się pojawić. Jeśli pojawia się blok AB^3, to musi tylko raz (inaczej $\psi(n) \geqslant 2 \cdot 0.27762 = 0.55524 > 0.47223$) i to na początku (inaczej $\psi(n)+\ln(\lambda(n)) \geqslant 0.27762+0.21194 = 0.48956 > 0.47223$). Gdyby pojawił się jakiś inny poza nim, to mielibyśmy $\psi(n) + \ln(\lambda(n)) \geqslant (0.27762 + 0.09185) + 0.13619 = 0.50566$, znowu zbyt wiele. Zatem w takim przypadku n musi mieć postać $1000101010\ldots$. Jednak jednocześnie musimy mieć $\ln(\lambda(n)) \leqslant 0.47223-\psi(n) \leqslant 0.19461$, zaś $\ln(\lambda(\mathsf{ABBBABABA})) = \ln(1+\phi^{-4} + \phi^{-6} + \phi^{-8}) \approx 0.20124$, więc takich przypadków jest skończenie wiele.

Zatem jedyne bloki o dodatnim ψ jakie mogą się pojawiać w n (czyli bloki więcej niż jednego zera), to AB^2. Oczywiście brak bloków oznacza, że n jest postaci $101010\ldots$, czyli F_k-1, z 5.1 wiemy zaś, że wtedy $\frac{\mathsf{P}(n)}{n} = \frac{F_{k+1}-1}{F_k-1} \to \phi$, więc nie tworzy to kontrprzykładu. To oznacza, że przynajmniej jeden taki blok istnieje. W szczególności $\psi(n) \geqslant 0.09185$, czyli $\ln(\lambda(n)) \leqslant 0.47223 - \psi(n) \leqslant 0.38038$. Ponadto $\ln(\lambda(\mathsf{ABABBA})) = \ln(1 + \phi^{-2} + \phi^{-5}) \approx 0.38671$, co ma zbyt dużą wartość, sprzeczność. Zatem zapis n musi zaczynać się od AB^2. Jeśli nie ma żadnych innych bloków tego typu, dostajemy tę samą strukturę, co do której już przeliczyliśmy, że granica wynosi tyle, ile chcemy.

Przyjmijmy więc, że istnieje jeszcze co najmniej jeden taki; wtedy $\psi(n) \geqslant 2 \cdot 0.09185 = 0.1837$, więc $\ln(\lambda(n)) \leqslant 0.47223 - 0.1837 = 0.28853$. Ponieważ $\ln(\lambda(\mathsf{ABBABABBA})) \approx 0.29827$, a to zbyt wiele, to drugi z tych bloków musi występować na drugiej pozycji. Skoro $\ln(\lambda(\mathsf{ABBA})) \approx 0.21194$ (korzystając z tabeli 2), to widzimy, że takie bloki mogą być tylko dwa; w przeciwnym razie $\psi(n) + \ln(\lambda(n)) \geqslant 3 \cdot 0.09185 + 0.21194 = 0.48749$, czyli zbyt wiele.

Ostatecznie więc n musi mieć strukturę $100100 \star \mathfrak{z}_k$ dla jakiegoś k. Stąd $n = F_{k+7} + F_{k+4} + F_{k+2} - 1$ (po dodaniu jedynki 100101 i k zer), zaś z 3.2

$$\mathsf{P}(n) = \mathsf{P}_0(100100)\mathsf{P}^1(\mathfrak{z}_k) + \mathsf{P}_1(100100)\mathsf{P}^0(\mathfrak{z}_k) - 1 = 19F_{k+2} + 7F_{k+1} - 1,$$

więc

$$\frac{\mathsf{P}(n)}{n} = \frac{19F_{k+2} + 7F_{k+1} - 1}{F_{k+7} + F_{k+4} + F_{k+2} - 1} \to \frac{19\phi + 7}{\phi^6 + \phi^3 + \phi} = \frac{19\phi + 7}{11\phi + 6} \approx 1.58593$$

To kończy dowód. □

Dla dosyć dużych wartości κ, powyższe metody pozwalają nam względnie efektywnie wyznaczyć i sprawdzić kandydatów na takie n, że $\mathsf{P}(n) \geqslant \kappa n$. Dla punktów stałych jednak $\kappa = 1$, więc zlogarytmowane twierdzenie A.1 przyjmuje postać

$$\psi(n) + \ln(\lambda(n)) \leqslant 1.01665,$$

i sytuacja nieco się komplikuje. Za pomocą samego spojrzenia na ψ mamy 42 przypadki; dorzucając do tego zerknięcie λ możemy tę liczbę ograniczyć, ale niezbyt bardzo. Zaczniemy od przypadku, w którym n zawiera blok pięciu zer.

Fakt A.1. 36 (w zapisie Zeckendorfa 10000010) jest jedynym punktem stałym zawierającym pięć zer z rzędu.

Dowód. Uwzględniając ψ za AB^5 oraz λ za $\mathsf{AB}^5\mathsf{A}$ dostajemy łącznie (korzystając z wcześniejszych tabel) 0.87006, czyli pozostało nam jeszcze 0.14659 „do wykorzystania". To oznacza, że jedyny inny blok o dodatnim psi jaki możemy mieć, to pojedynczy AB^2. Bez względu na to czy wystąpi on, czy nie, cząstka AB^5 musi być zawarta na początku, inaczej $\ln(\lambda(n)) \geqslant 0.21194$, i razem z $\psi(n)$ dostaniemy zbyt wiele.

Zaczniemy od przypadku, gdy nie ma innych bloków ψ-dodatnich, czyli zapis n to $100000 \star \mathfrak{z}_k$. Wtedy $n = F_{k+7} + F_{k+2} - 1$ oraz, z Twierdzenia 3.2,

$$\mathsf{P}(n) = 11F_{k+2} + 2F_{k+1} - 1,$$

więc $\mathsf{P}(n) = n$ implikuje $F_{k+7} + F_{k+2} = 11F_{k+2} + 2F_{k+1}$. Jednak możemy zapisać F_{k+7} jako $F_{k+6} + F_{k+5} = 2F_{k+5} + F_{k+4} = \ldots = 8F_{k+2} + 5F_{k+1}$. Otrzymujemy więc $9F_{k+2} + 5F_{k+1} = 11F_{k+2} + 2F_{k+1}$, czyli $3F_{k+1} = 2F_{k+2}$. Stąd widzimy, że $k = 2$ – istotnie, $F_{k+2} = \frac{3}{2}F_{k+1}$ implikuje $F_k = F_{k-1} = \frac{1}{2}F_{k+1}$, zaś jedyne dwie kolejne liczby Fibonacciego o równych wartościach dostajemy dla $k - 1 = 1$, czyli $k = 2$.

Pozostaje przypadek, gdy mamy gdzieś jeszcze blok AB^2. Wiemy, że $\operatorname{tr}(AB^5A)(AB^5A)^T = 146$, mamy $\psi(\mathsf{AB}^5\mathsf{A}) \geqslant -\ln \frac{\sqrt{146}}{\phi^7} \approx 0.87668$, co razem z ψ dla pozostałego bloku (0.09185) oraz z $\ln(\lambda)$ (równym 0.05423) daje 1.02276, czyli za dużo – to nie możemy znaleźć rozłącznych fragmentów $\mathsf{AB}^5\mathsf{A}$ i AB^2, jednym słowem bloki te muszą wystąpić obok siebie. Jednak $\operatorname{tr} AB^5AB^2 = 774$, więc $\psi(\mathsf{ABBBBBABB}) \geqslant \frac{\sqrt{774}}{\phi^9} \approx 1.00512$, co razem z uwzględnieniem λ da więcej niż próg 1.01665. To kończy dowód.

$\square$

W dowodzie można zobaczyć kolejną koncepcję, którą będziemy stosować – możemy brać ψ z obszarów większych niż jeden blok, co da czasami większą wartość. Trzeba jednak wtedy uważać, by były one nadal rozłączne. Najpierw jednak przeanalizujmy możliwe przypadki, które zostają po samym uwzględnieniu δ. Z Faktu A.1 wystarczy przejmować się występowaniem bloków AB^2, AB^3, AB^4. Jeśli występuje ten ostatni, to $\ln(\lambda(n))$ jest (z tabelki 2) równy co najmniej 0.08633, więc $\psi(n) \leqslant 0.93032$. Korzystając z tabelki 1 widzimy, że AB^4 jest tylko jedno. Jeśli mamy a bloków AB^2 oraz b postaci AB^3, dostajemy w ten sposób nierówność $0.09185a + 0.27762b \leqslant 0.40459$, do której rozwiązaniami będą $b = 1$ i $a \leqslant 1$ oraz $b = 0$ i $a \leqslant 4$ – łącznie siedem przypadków.

Jeśli AB^4 nie ma, to miejmy a bloków AB^2 oraz b bloków AB^3. Jeśli $b > 0$, to $\ln(\lambda(n)) \geqslant 0.13619$, więc $0.09185a + 0.27762b \leqslant \psi(n) \leqslant 0.88046$. Ta nierówność ma rozwiązania:

- $b = 3$, $a = 0$
- $b = 2$, $a = 0,\ 1,\ 2,\ 3$
- $b = 1$, $0 \leqslant a \leqslant 6$

To 12 rozwiązań. Dla $b = 0$ dostajemy $\ln(\lambda(n)) \geqslant 0.21194$, więc $0.09185a \leqslant \psi(n) \leqslant 0.80471$, czyli $0 \leqslant a \leqslant 8$ – kolejnych dziewięć przypadków. Łącznie dostajemy ich więc 28. Aby zmniejszyć tę liczbę dalej, skorzystamy z następujących wartości ψ (a konkretniej ich szacowań wynikających z $||M||_2 \leqslant \operatorname{tr} MM^T$):

$\mathfrak{s}$	$\psi(\mathfrak{s})$
ABBABB	0.21372
ABBAB	0.1085
ABBBABBB	0.62922
ABBBABB	0.42822
ABBBAB	0.31644
ABBBBABBB	0.90215
ABBBBABB	0.69839
ABBBBAB	0.58241

Tabela 3: Więcej wartości funkcji ψ.

Za pomocą tych informacji możemy odrzucić jeszcze więcej przypadków.

a) Przyjmijmy, że n ma siedem bloków AB^2. Wtedy

$$\ln(\lambda) \geqslant \ln(1 + \phi^{-3} + \phi^{-6} + \phi^{-9} + \phi^{-12}) \approx 0.26854$$

Spróbujmy pogrupować bloki AB^2 w pary tak, by bloki w każdej parze ze sobą sąsiadowały. Zrobimy to rozpatrując je od lewej: jeśli jeszcze nie przyporządkowaliśmy aktualnego bloku, a bezpośrednio po nim następuje znowu AB^2, to grupujemy je w pary; w przeciwnym razie nie robimy razem. Łatwo zauważyć, że po dowolnym niesparowanym bloku AB^2 następuje AB, chyba że jest to blok końcowy. Stąd, jeśli mamy k par, dostajemy szacowanie

$$\begin{aligned}\psi(n) \geqslant k\psi(\mathsf{ABBABB}) + (6-2k)\psi(\mathsf{ABBAB}) + \psi(\mathsf{ABB}) = \\ = 0.21372k + 0.1085(6-2k) + 0.09185\end{aligned}$$

to oszacowanie jest funkcją liniową o ujemnym współczynniku przy k, więc opłaca nam się, by było ono jak największe, to znaczy równe 3. Dostajemy sumę $\psi + \lambda$ równą 1.00155, brakuje więc 0.0151.

Jeśli żaden z bloków AB^2 nie występuje na końcu, to 0.09185 w szacowaniu możemy zastąpić przez jedno 0.1085, co daje nam dodatkowe 0.01665, o całą jedną tysięczną więcej niż potrzebujemy. Pozostaje przypadek, gdy taki blok na końcu występuje. Spójrzmy do dowodu twierdzenia 5.4. Szacowaliśmy tam $||Mv||_2$ przez $||M||_2||v||_2$, czyli wzrost długości wektora przez najbardziej optymistyczny przypadek. My jednak znamy macierz, która „rozpoczyna" działanie na tym wektorze – jest to $AB^2 = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, zatem $||AB^2v||_2 = ||(3,4)^T||_2 = 5$. „Rzeczywisty" deficyt będzie tu wynosił zatem nie wartość $\delta(\mathsf{ABB})$, którą policzyliśmy wcześniej, to znaczy $\phi^{-3}\sqrt{\frac{15+\sqrt{221}}{2}}$, a $\frac{||AB^2v||}{||v||} = \frac{5}{\sqrt{2}}$, co jednocześnie daje ψ równe $-\ln \frac{5}{\phi^3\sqrt{2}} \approx 0.18077$. To daje nam oczywiście zwiększenie oszacowania łącznego ψ o 0.08892, czyli więcej niż potrzebujemy.

Powyższy rezultat jest o tyle ciekawy, że w pewien sposób optymalny – 4656039 w zapisie Zeckendorfa to

$$100100101001010100101001001010 10$$

zatem zawiera 6 bloków AB^2 i jest punktem stałym P.

b) Załóżmy, że mamy trzy bloki ABBB. Jeśli dwa takie bloki wystąpią obok siebie, to możemy oszacować ψ przez $\psi(\mathsf{ABBBABBB}) + \psi(\mathsf{ABBB})$, zaś korzystając z Tabeli 2 odnośnie wartości λ, dostajemy łącznie $0.62922 + 0.27762 + 0.13619 = 1.04303$, czyli zbyt wiele.

   Jeśli zaś takich dwóch bloków nie ma, to znaczy że co najmniej dwa razy wystąpi podsłowo ABBBAB. Ponieważ $2\psi(\mathsf{ABBBAB})$ jest nawet większe niż $\psi(\mathsf{ABBBABBB})$, dostajemy sprzeczność także w tym przypadku.

c) Niech bloki ψ-dodatnie to pojedynczy ABBB oraz sześciokrotnie ABB. Jeśli nasze słowo nie będzie się zaczynało od AB^3, to $\ln\lambda + \psi \geqslant 0.21194 + 0.27762 + 6 \cdot 0.09185 = 1.04066$. W takim razie musi się ono zaczynać od ABBB. Powtarzając rozumowanie z grupowaniem w pary z przypadku a), dostajemy szacowanie

$$\psi + \ln\lambda \geqslant (\psi(\mathsf{ABBB}) + 2\cdot\psi(\mathsf{ABBABB}) + \psi(\mathsf{ABBAB}) + \psi(\mathsf{ABB})) + \\ + 0.13619 = 1.0416$$

(gdzie skorzystaliśmy z tego, że dwa niesparowane ABB, z czego jedno na końcu, dają mniejszą wartość niż dwa sparowane).

d) Tym razem niech blokami o dodatnim ψ będą AB^4, AB^3, AB^2. Jeśli AB^4 nie będzie na początku, dostaniemy łącznie $\psi + \lambda \geqslant (0.52573 + 0.27762 + 0.09185) + 0.13619 = 1.03139$. Jeśli będzie, to sprawdzamy przypadki względem tego co za nim:

- Jeśli AB, to

$$\psi + \ln\lambda \geqslant \psi(\mathsf{ABBBBAB}) + \psi(\mathsf{ABBB}) + \psi(\mathsf{ABB}) + \ln\lambda \geqslant$$
$$\geqslant 0.58241 + 0.27762 + 0.09185 + 0.08633 = 1.03821$$

- Jeśli ABB, to analogicznie

$$\psi + \ln\lambda \geqslant \psi(\mathsf{ABBBBABB}) + \psi(\mathsf{ABBB}) + \ln\lambda \geqslant$$
$$\geqslant 0.69839 + 0.27762 + 0.08633 = 1.06234$$

- Wreszcie jeśli ABBB, to podobnie

$$\psi + \ln\lambda \geqslant \psi(\mathsf{ABBBBABBB}) + \psi(\mathsf{ABB}) + \ln\lambda \geqslant$$
$$\geqslant 0.90215 + 0.09185 + 0.08633 = 1.08033$$

e) Jeśli bloki ψ-dodatnie jakie mamy, to AB^4 i cztery razy AB^2, to znowu rozważamy przypadki

- Jeśli AB^4 nie jest na początku, to

$$\psi + \ln\lambda \geqslant 0.52573 + 4 \cdot 0.09185 + 0.21194 = 1.10507$$

- Jeśli jest i następuje po nim AB, to

$$\psi + \ln\lambda \geqslant \psi(\mathsf{ABBBBAB}) + 4 \cdot \psi(\mathsf{ABB}) + \ln\lambda \geqslant$$
$$\geqslant 0.58241 + 4 \cdot 0.09185 + 0.08633 = 1.03614$$

- Jeśli następuje po nim ABB, to

$$\psi + \ln\lambda \geqslant \psi(\mathsf{ABBBBABB}) + 3 \cdot \psi(\mathsf{ABB}) + \ln\lambda \geqslant$$
$$\geqslant 0.69839 + 3 \cdot 0.09185 + 0.08633 = 1.06027$$

Fakt A.2. Jeśli AB^4 jest jedynym blokiem ψ-dodatnim w n spełniającym $\mathsf{P}(n) = n$, to $n = 78$ (które w zapisie Zeckendorfa to 101000010

Dowód. Niech zapis n będzie postaci $\mathfrak{z}_{2s} \star \mathsf{ABBBB} \star \mathfrak{z}_t$. Wtedy $n = F_{2s+t+7} - F_{t+5} + F_{t+2} - 1$, gdyż po dodaniu jedynki oraz F_{t+5} (odpowiadającego za pozycję na której stoi pierwsze B w środkowym segmencie) suma nam się złoży do liczby o dwóch niezerowych cyfrach. Równoważnie liczbę tę można zapisać jako $F_{2s+t+7} - 2F_{t+3} - 1$. Ponadto

$$
\begin{aligned}
\mathsf{P}(n) = \begin{pmatrix}1 & 1\end{pmatrix} M(\mathfrak{z}_{2s}) \begin{pmatrix}1 & 4\\ 1 & 5\end{pmatrix} M(\mathfrak{z}_t) \begin{pmatrix}1\\ 1\end{pmatrix} - 1 = \\
= \begin{pmatrix}F_{2s+1} & F_{2s+2}\end{pmatrix} \begin{pmatrix}1 & 4\\ 1 & 5\end{pmatrix} \begin{pmatrix}F_{t+1}\\ F_{t+2}\end{pmatrix} - 1 = \\
= \begin{pmatrix}F_{2s+3} & 4F_{2s+3} + F_{2s+2}\end{pmatrix} \begin{pmatrix}F_{t+1}\\ F_{t+2}\end{pmatrix} - 1 = \\
= F_{2s+2}F_{t+2} + F_{2s+3}(4F_{t+2} + F_{t+1}) - 1 = F_{2s+2}F_{t+2} + F_{2s+3}(F_{t+3} + 3F_{t+2}) - 1
\end{aligned}
$$

dostajemy więc równanie

$$F_{2s+t+7} - 2F_{t+3} = F_{2s+2}F_{t+2} + F_{2s+3}(F_{t+3} + 3F_{t+2}) - 1$$

Z tożsamości $F_{k+l} = F_k F_{l+1} + F_{k-1} F_l$, którą można udowodnić na przykład ze wzoru Bineta (lub po prostu indukcją) możemy zapisać F_{2s+t+7} jako $F_{2s+4}F_{t+4} + F_{2s+3}F_{t+3} = (F_{2s+3} + F_{2s+2})(F_{t+3} + F_{t+2}) + F_{2s+3}F_{t+3}$. Równanie przybiera więc postać

$$
\begin{aligned}
(F_{2s+3} + F_{2s+2})(F_{t+3} + F_{t+2}) - 2F_{t+3} + F_{2s+3}F_{t+3} = \\
= F_{2s+2}F_{t+2} + F_{2s+3}(F_{t+3} + 3F_{t+2})
\end{aligned}
$$

lub po skróceniu części wyrazów

$$F_{2s+3}F_{t+3} + F_{2s+2}F_{t+3} = 2F_{t+3} + 2F_{2s+3}F_{t+2},$$

czyli $F_{2s+4}F_{t+3} = 2F_{t+3} + 2F_{2s+3}F_{t+2}$. Jeśli $t = 0$, dostajemy $F_{2s+2} = 2$, co jest niemożliwe ($F_3 = 2$ ma nieparzysty indeks). Przyjmijmy $t \geqslant 1$. Rozpisując $F_{2s+4} = F_{2s+3} + F_{2s+2}$ i $F_{t+3} = F_{t+2} + F_{t+1}$ dostaniemy

$$F_{2s+3}F_{t+1} + F_{2s+2}F_{t+2} + F_{2s+2}F_{t+1} = 2F_{t+3} + F_{2s+3}F_{t+2}$$

Ponieważ mamy szacowanie $F_{2s+3}F_{t+1} + F_{2s+2}F_{t+2} \geqslant F_{2s+3}F_{t+2}$ (równoważne $\frac{F_{t+1}}{F_{t+2}} + \frac{F_{2s+2}}{F_{2s+3}} \geqslant 1$, co jest prawdą jako iż oba te ułamki są $\geqslant \frac{1}{2}$ (skoro $t > 0$)), dostajemy $F_{2s+2}F_{t+1} \leqslant 2F_{t+3}$, czyli $F_{2s+2} \leqslant 2\frac{F_{t+3}}{F_{t+1}}$. Ponieważ $F_{t+3} = 2F_{t+1} + F_t \leqslant 3F_{t+1}$, prawa strona to co najwyżej 6, stąd $s \leqslant 1$.

Wróćmy do postaci $F_{2s+4}F_{t+3} = 2F_{t+3} + 2F_{2s+3}F_{t+2}$. Jeśli $s = 0$, dostajemy $F_{t+3} = 4F_{t+2}$, co jest oczywiście niemożliwe. Jeśli $s = 1$, to $6F_{t+3} = 10F_{t+2}$. Stąd $F_{t+3} = \frac{5}{3}F_{t+2}$, więc $F_{t+1} = \frac{2}{3}F_{t+2}$, i kontynuując to rozumowanie dostajemy $F_t = F_{t-1}$, czyli $t = 2$. Ostatecznie $(s,t) = (1,2)$ jest jedynym rozwiązaniem, dla którego dostajemy $n = 78$.

$\square$

Pamiętając również, że brak bloków ψ-dodatnich oznacza $n = F_k - 1$ i $\mathsf{P}(n) > n$, dostajemy obiecaną redukcję do dwudziestu przypadków.

Na koniec wróćmy do dowodu Twierdzenia 5.6 i rozważań na temat możliwych wartości P.

Dalszy ciąg dowodu Twierdzenia 5.6. Będziemy chcieli policzyć liczbę podciągów $\mathsf{AB}^k\mathsf{AB}^l\mathsf{AB}^m$. Wiemy, że jest to o jeden mniej niż

$$\begin{pmatrix}1 & 1\end{pmatrix}\begin{pmatrix}1 & k\\ 1 & k+1\end{pmatrix}\begin{pmatrix}1 & l\\ 1 & l+1\end{pmatrix}\begin{pmatrix}1 & m\\ 1 & m+1\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix},$$

co po wymnożeniu (i odjęciu jedynki) przyjmuje postać

$$2klm + 4kl + 4km + 3lm + 6k + 6l + 4m + 4 \tag{1}$$

Przypomnijmy, że n jakie nam zostały do uzyskania, mają postać $2^t - 3$ z $t \geqslant 7$ oraz $3 \cdot 2^t - 3$ z $t \geqslant 5$ (pozostałe n tych postaci wykluczaliśmy wśród małych przypadków). Są to liczby nieparzyste, zaś powyższe wyrażenie przystaje do lm modulo 2, chcielibyśmy więc, by l oraz m były nieparzyste – można by więc podstawić $l = 2l' + 1$ oraz $m = 2m' + 1$, co okazuje się iż niewiele upraszcza (ułatwia jednak zgadywanie jakie przypadki mogą być interesujące).

Podstawmy $l = 1$. Nasza liczba podciągów przyjmuje postać $n = 6km + 10k + 7m + 10$. Możemy równoważnie przekształcić tę równość do $3n + 5 = 18km + 30k + 21m + 35 = (6k+7)(3m+5)$. Jeśli $n = 3 \cdot 2^t - 3$, to $3n + 5 = 9 \cdot 2^t - 4$. Spójrzmy na przypadek parzystego $t =: 2w$. Dostajemy

$$3n + 5 = (3 \cdot 2^w)^2 - 2^2 = (3 \cdot 2^w - 2)(3 \cdot 2^w + 2) = (3 \cdot 2^{w-1} - 1)(3 \cdot 2^{w+1} + 1)$$

Zatem biorąc $m = 2^{w-1} - 2$ oraz $k = 2^w - 1$ dostajemy to co chcemy (przy czym $w \geqslant 3$, więc $k > 0$ i $m \geqslant 0$ tak jak chcemy).

Wróćmy do wyrażenia (1) i podstawmy tym razem $k = 1$. Otrzymujemy $n = 5lm + 10l + 8m + 10 = (5l + 8)(m + 2) - 6$. Zatem biorąc $n = 3 \cdot 2^t - 3$ w przypadku t nieparzystego, dostajemy

$$3(2^t + 1) = (5l + 8)(m + 2)$$

Widzimy, że jeśli $2^t \equiv 2 \pmod 5$ i $t > 1$, możemy wziąć $m = 1$ i $5l + 8 = 2^t + 1$ – to pozbywa się przypadku $t \equiv 1 \pmod 4$. W przypadku $t \equiv 3 \pmod 4$ będziemy chcieli wziąć $m = 7$ oraz $5l + 8 = \frac{2^t+1}{3}$. Ta druga równość jest możliwa do spełnienia, ponieważ skoro $2 \nmid t$, to $3 \mid 2^t + 1$, zaś $t \equiv 3 \pmod 4$ oznacza $2^t \equiv 3 \pmod 5$, więc $\frac{2^t+1}{3} \equiv 3 \pmod 5$ (oraz $\frac{2^t+1}{3} > 8$, gdyż $t > 3$).

Ostatecznie więc pozostaje nam tylko przypadek $n = 2^t - 3$. Podstawmy w (1) $m = l = 3$, dostając $n = 48k + 61$, czyli $2^t = 48k + 64$, a zatem $2^{t-4} = 3k + 4$. Takie k istnieje dla t parzystych (i jest dodatnie dla $t \geqslant 7$). Podobnie podstawiając $l = 1$, $m = 5$ dostaniemy $n = 40k + 45$, więc $2^{t-3} = 5k + 6$ i odpowiednie k znajdziemy, o ile $t \equiv 3 \pmod 5$ i $t > 3$. Zatem faktycznie jedyny przypadek jaki nam zostaje, to $n = 2^t - 3$ dla $t \equiv 1 \pmod 4$, lub równoważnie $n = 2 \cdot 16^t - 3$.

□

Być może ten pozostały przypadek także da się pokonać skończoną liczbą ciągów arytmetycznych. Problemem okazuje się, że każde słowo bez dwóch kolejnych liter A (równoważnie, liczba w systemie Zeckendorfa) o $8189 = 2^{13} - 3$ podciągach zawiera co najmniej cztery litery A – zatem poszukiwania należałoby prowadzić z czterema zmiennymi. Nawet częściowe uogólnienie rezultatów dla $509 = 2^9 - 3$ daje dosyć mało zadowalające wyniki – jedyne rozwiązania to $(k, l, m) = (2, 5, 9)$ oraz $(k, l, m) = (1, 19, 3)$; „uwalniając” jedną z tych zmiennych (to znaczy podstawiając wartości dwóch pozostałych do (1)) dostaniemy jakiś ciąg arytmetyczny tak jak robiliśmy to wcześniej, jednak różnice tych ciągów[10] to na przykład 13, 25 czy 77. To pozwoli nam wykluczyć przypadek t odpowiednio co trzeciego, co piątego i co dwudziestego trzeciego. Jednak nie daje to większego postępu w walce z przypadkiem ogólnym.

Być może zapisanie (1) jako $n = (2k + 3)(l + 2)(m + 2) - (2k + 3) - 2(m + 2) - 1$ jest dobrym pomysłem, ale nie udało mi się go doprowadzić do jakiegokolwiek punktu, który stanowiłby istotny przełom w rozwiązaniu.

[10]Po wyciągnięciu przed nawias potęgi dwójki, co w naszym przypadku nic nie zmienia.

B Problemy otwarte

Sumienny lekarz umiera razem z chorym, jeśli nie potrafi go wyleczyć.

„Łysa śpiewaczka”
Eugene Ionesco

Powyższa praca pełna jest rozważań niedokończonych lub nierozpoczętych; w tej sekcji zbiorę je wszystkie. Stanowią one naturalne kierunki rozwoju względem koncepcji, które zaprezentowałem wyżej, natomiast niewątpliwie pytań, które można postawić, jest o wiele więcej.

- Przede wszystkim – czy odpowiedniki powyższych rozważań da się przedstawić dla słów nad alfabetem o więcej niż dwóch elementach? Jako iż już sam przypadek dwóch liter ma dosyć obszerną teorię, ani nie poruszałem tego tematu w pracy, ani też szczególnie go nie badałem, natomiast wydaje się że wiele można tu zrobić.
- Górna granica długości słowa o n podciągach – nasz rezultat $O(\sqrt{n})$ jak widzieliśmy, prawdopodobnie da się poprawić do $O(\log n)$, jednak przepaść między tymi szacowaniami jest tak wielka, że prawdopodobnie dałoby się ją choćby częściowo zredukować za pomocą elementarnych metod.
- Dowód Twierdzenia 3.2 bez użycia indukcji – mimo poszukiwań, nie udało mi się znaleźć takiej drogi jego wykazania, która opierałaby się tylko na zliczaniu odpowiednich podciągów i znajdywaniu bijekcji między zbiorami opisywanymi przez obie strony równania.
- Najwięcej pytań bez odpowiedzi pozostało w kwestii funkcji P na $\mathbb{N}$. Nie wiemy jak długie mogą być cykle, i czy jest ich nieskończenie wiele.
- Nie wiemy nawet, czy jest nieskończenie wiele punktów stałych. Dalsze ograniczenie puli możliwych typów takich punktów (oraz dowód, że punktów danego typu jest skończenie/nieskończenie wiele), jest jednym z możliwych kierunków badań.
- Obliczenia komputerowe sugerują, że twierdzenie 5.6 da się ulepszyć do stwierdzenia, że każda liczba większa od 61 leży w obrazie P. Do tego jednak, prawdopodobnie, potrzeba więcej niż trzech bloków (dla 8189 wszystkie rozwiązania zawierają co najmniej cztery litery A).

- Bardzo naturalną kwestią, której w zasadzie nie rozważałem, jest czy $1 \to 2 \to 4 \to \ldots \to F_n - 1$ to jedyna trajektoria P która nie wpada w cykl.

Literatura

[1] Piotr Chrząstowski-Wachtel, *Bity w szufladkach*, Delta, grudzień 2016, `http://www.deltami.edu.pl/temat/matematyka/teoria_liczb/2016/11/25/Bity_w_szufladkach/`

[2] Henryk Iwaniec, *On the problem of Jacobsthal*, Demonstratio Mathematica, 1978, doi:10.1515/dema-1978-0121.

[3] https://kconrad.math.uconn.edu/blurbs/grouptheory/SL(2,Z).pdf

[4] Jean Bourgain, Alex Kontorovich, *On Zaremba's conjecture*, https://annals.math.princeton.edu/wp-content/uploads/annals-v180-n1-p03-s.pdf

[5] L. E. J. Brouwer, *On the structure of perfect sets of points*, https://www.dwc.knaw.nl/DL/publications/PU00013496.pdf