Niemożliwy skrót

Damian NIWIŃSKI[*]

Ten list uczyniłem dłuższym tylko dlatego, że nie miałem dość czasu, by napisać go krócej. Usprawiedliwienie, jakie Blaise Pascal wkłada w swój XVI *List prowincjalny*, wyraża intuicję, iż zapisanie jakiejś myśli zwięźle może być bardziej czasochłonne niż zapisanie jej rozwlekle. Umiejętność skrótu bywa przejawem geniuszu. Tadeusz Boy-Żeleński odnotowuje następujący przykład sztuki translatorskiej Stanisława Wyspiańskiego. Pierwsze zdanie tragedii Pierre'a Corneille'a *Cyd* brzmiałoby w dosłownym przekładzie z francuskiego na polski:

> *Elwiro, czy zupełnie szczerze powtórzyłaś mi wszystko? Czy nie ukrywasz nic z tego, co powiedział ojciec?*

W przekładzie Wyspiańskiego fragment ten brzmi

> *Więc mówił...?*

Zostawiamy tymczasem poezję, by przyjrzeć się zagadnieniu skrótu w dziedzinie matematyki. Na przykład, jakie jest najkrótsze przedstawienie danej liczby naturalnej? Pytanie nie jest całkiem precyzyjne (co to jest przedstawienie?), ale ma pewien potencjał sensu. Jasne jest w szczególności, że odpowiedź zależy od własności danej liczby bardziej niż od jej rozmiaru. Na przykład, wypisanie cyfr dziesiętnego rozwinięcia liczby

$$N = 10^{10^{10}}$$

przekroczyłoby ramy tego artykułu, a nawet zapewne wszystkich numerów *Delty* (dla porównania: liczbę atomów we Wszechświecie szacuje się „jedynie" przez 3^{200}), ale przecież przedstawiliśmy ją powyżej jednoznacznie. W konsekwencji niedługie przedstawienie będzie miała też na pozór bardziej skomplikowana liczba

$$\underbrace{31415926535897932384626433832 79\ldots\ldots\ldots}_{N+1}$$

utworzona przez $N+1$ początkowych cyfr rozwinięcia dziesiętnego liczby π, którą możemy zapisać w postaci $\lfloor \pi \cdot 10^N \rfloor$. Czytelnik zauważy oczywiście, że odwołujemy się tutaj do pewnych „kodów kulturowych" (notacja potęgowania, definicja liczby π). O tym, że droga ta może być ryzykowna, świadczy tzw. *paradoks Berry'ego* podany przez Bertranda Russella (G.G. Berry, któremu Russell przypisał autorstwo tego paradoksu, był bibliotekarzem w oksfordzkiej *Bodleian Library*):

> *najmniejsza liczba naturalna n, której nie da się opisać w języku polskim przez mniej niż 1000 symboli*

właśnie została tak opisana!

Aby uniknąć paradoksu, spójrzmy na możliwe przedstawienie liczb naturalnych globalnie, jak na funkcję $\alpha : \mathbb{N} \to A^*$, gdzie A^* jest zbiorem wszystkich słów, jakie można utworzyć z liter pewnego skończonego alfabetu A. Dla jednoznaczności potrzeba, by funkcja α była różnowartościowa. Interesować nas będzie długość $|\alpha(n)|$ słowa $\alpha(n)$. Mamy, na przykład, standardowe przedstawienia liczb w k-arnym systemie pozycyjnym (np. binarnym lub dziesiętnym), $\alpha : \mathbb{N} \to \{0, 1, \ldots, k-1\}^*$, gdzie $|\alpha(n)| = \lfloor \log_k n \rfloor + 1$. Mogłoby się wydawać, że w każdej liczbie dopatrzymy się jakiejś „regularności" (czyż nie uruchamiamy inwencji, by zapamiętać kod PIN?), która pozwoli zapisać ją istotnie krócej. Jednak prosty rachunek wykaże pewną barierę.

Lemat o nieskracalności. *Dla dowolnej różnowartościowej funkcji $\alpha : \mathbb{N} \to A^*$ istnieje nieskończenie wiele $n \in \mathbb{N}$, dla których $|\alpha(n)| \geqslant \lfloor \log_r n \rfloor$, gdzie r jest liczbą elementów zbioru A.*

Dowód. Zauważmy najpierw, że słów krótszych niż k jest

$$1 + r + r^2 + \ldots + r^{k-1} = \frac{r^k - 1}{r - 1} < r^k.$$

Przyjmując $k = \lfloor \log_r m \rfloor$, widzimy, że dla każdego m musi istnieć pewna liczba $hard(m) < m$, dla której

$$|\alpha(hard(m))| \geqslant \lfloor \log_r m \rfloor.$$

Wybierzmy najpierw m, dla którego $\lfloor \log_r m \rfloor > |\alpha(0)|$. Wtedy

$$|\alpha(hard(m))| \geqslant \lfloor \log_r m \rfloor \geqslant \lfloor \log_r hard(m) \rfloor$$

(ostatnia nierówność z nieostrej monotoniczności funkcji $\lfloor \log_r x \rfloor$). Połóżmy $m_0 = hard(m)$.

Przypuśćmy teraz, że wybraliśmy już ℓ różnych liczb $m_0, m_1, \ldots, m_{\ell-1}$, z których każda spełnia $|\alpha(m_i)| \geqslant \lfloor \log_r m_i \rfloor$. Wybierzmy m tak, by

$$(*) \qquad \lfloor \log_r m \rfloor > \max\left(|\alpha(m_0)|, \ldots, |\alpha(m_{\ell-1})|\right).$$

Ponownie, dla pewnego $hard(m) < m$ mamy $|\alpha(hard(m))| \geqslant \lfloor \log_r m \rfloor \geqslant \lfloor \log_r hard(m) \rfloor$. Z nierówności $(*)$ mamy $hard(m) \notin \{m_0, m_1, \ldots, m_{\ell-1}\}$. Kładziemy więc $m_\ell = hard(m)$.

Utworzony w ten sposób ciąg $m_0, m_1, \ldots$ potwierdza tezę Lematu. □

Pozwolimy sobie teraz na dygresję i pokażemy, że Lemat o nieskracalności dostarcza jednego z wielu możliwych argumentów na

Twierdzenie (Euklides)**.** *Istnieje nieskończenie wiele liczb pierwszych.*

Dowód. Przypuśćmy, że przeciwnie – pierwsze są jedynie liczby $p_0, p_1, \ldots, p_{k-1}$. A zatem każdą liczbę naturalną można przedstawić w postaci

$$n = p_0^{a_{n,0}} \cdot p_1^{a_{n,1}} \cdot \ldots \cdot p_{k-1}^{a_{n,k-1}},$$

dla pewnych $a_{n,0}, a_{n,1}, \ldots, a_{n,k-1} \in \mathbb{N}$. To pozwala nam określić przedstawienie $\alpha : \mathbb{N} \to \{0, 1, 2\}^*$

$$\alpha(n) = bin(a_{n,0})\, 2\, bin(a_{n,1})\, 2\, \ldots\, 2\, bin(a_{n,k-1}),$$

gdzie $bin(x)$ oznacza binarne przedstawienie liczby x. Mamy $|bin(x)| \leqslant \lfloor \log_2 x \rfloor + 1$, a z drugiej strony $a_{n,i} \leqslant \log_2 n$, bo $p_i \geqslant 2$. A zatem przedstawienie α spełnia

$$|\alpha(n)| \leqslant k \cdot (\lfloor \log_2 \log_2 n \rfloor + 2).$$

Z Lematu wynika, że dla nieskończenie wielu n

$$k \cdot (\lfloor \log_2 \log_2 n \rfloor + 2) \geqslant \lfloor \log_3 n \rfloor,$$

co jest, oczywiście, nie do pogodzenia z asymptotycznym zachowaniem występujących tu funkcji. A więc hipoteza skończoności zbioru liczb pierwszych była błędna. □

[*]Instytut Informatyki, Uniwersytet Warszawski

Powróćmy do postawionego na wstępie pytania o najkrótszy opis liczby n. Widzieliśmy już, że każde przedstawienie ma przykłady trudno skracalne, a z drugiej strony drastyczny skrót jest czasem możliwy. Zauważmy jednak, że rozważanie dowolnej funkcji różnowartościowej $\alpha : \mathbb{N} \to A^*$ jest nieco za ogólne, oczekujemy przecież, by z przedstawienia $\alpha(n)$ dało się odtworzyć n. Ściślej mówiąc, interesują nas przedstawienia α dane razem z *algorytmem*, który na podstawie $\alpha(n)$ oblicza n w jakimś zrozumiałym dla nas przedstawieniu (np. dziesiętnym). W pewnym sensie $\alpha(n)$ stanowi więc *program*, jaki może posłużyć do obliczenia n.

Idąc tym tropem, ustalmy sobie jakiś język programowania (np. Pascal lub C). Zachęcamy Czytelnika, by dla rozgrzewki napisał w swoim ulubionym języku program generujący wspomnianą wyżej liczbę $\lfloor \pi \cdot 10^N \rfloor$. (Nie radzimy go jednak uruchamiać...)

Ogólnie, dla dowolnej liczby n, niech P_n będzie programem o *najmniejszej* długości, który bez żadnych dodatkowych danych generuje liczbę n; jeśli takich programów jest więcej, wybieramy pierwszy w porządku leksykograficznym. Funkcja $\alpha : n \mapsto P_n$ zależy wprawdzie od wyboru języka programowania, jednak z ogólnej teorii obliczalności wynika, że długości programów wskazywanych przez funkcje dla sensownych języków różnią się co najwyżej o stałą (zależną od tych języków, ale nie od n).

Powyższe przedstawienie liczb naturalnych wprowadził Andriej N. Kołmogorow w badaniach nad losowością (Kołmogorow użył jako języka programowania abstrakcyjnego formalizmu maszyn Turinga). Z Lematu o nieskracalności wynika bowiem, że dla nieskończenie wielu n jest

$$|P_n| \geqslant \lfloor \log_r n \rfloor,$$

gdzie r jest rozmiarem alfabetu, jakiego używamy w naszym języku programowania. Można z grubsza powiedzieć, że dla takich liczb optymalnym (lub prawie optymalnym) rozwiązaniem jest banalny program w rodzaju *write*(n). Liczby te są „nieskracalne" z powodu braku jakiejkolwiek regularności, a więc *losowe*. Funkcja $n \mapsto |P_n|$, zaproponowana przez Kołmogorowa jako miara *losowości*, jest dziś powszechnie nazywana *złożonością Kołmogorowa*.

Subtelniejsza analiza dowodu Lematu pokazuje, że liczby trudno skracalne dominują pod względem gęstości. Paradoks polega na tym, że trudno jest wygenerować konkretne przykłady właśnie ze względu na losowy charakter tych liczb.

Złożoność Kołmogorowa rozwiązuje w pewnym sensie problem najkrótszego opisu, ma jednak pewną wadę, która ogranicza jej praktyczne zastosowanie. W pewnym sensie „dopada" nas tu paradoks Berry'ego.

Twierdzenie (Kołmogorow)**.** *Funkcja $n \mapsto P_n$ jest nieobliczalna, tzn. nie da się jej obliczyć żadnym algorytmem.*

Szkic dowodu. Zakładając, że mamy taki algorytm, możemy dalej skonstruować algorytm, który dla danego n znajduje najmniejsze M, takie że $|P_M| \geqslant n$; nazwijmy je M_n. Niech P będzie programem (z jedną zmienną wolną), który realizuje ten algorytm. Jeśli teraz ustalimy liczbę n i podstawimy ją w programie P za zmienną wolną, otrzymamy program (powiedzmy) Q_n, generujący liczbę M_n. Oszacujmy jego długość. Zakładając, że n jest dane w postaci binarnej, otrzymujemy

$$|Q_n| \leqslant (\lfloor \log_2 n \rfloor + 1) + |P| + \Delta,$$

gdzie stała Δ jest odpowiedzialna za podstawienie wartości liczbowej za zmienną. (W tym miejscu odwołujemy się do składni języka programowania.) Dla dostatecznie dużych n prawa strona tej nierówności jest ostro mniejsza od n, co daje nam nierówność $|Q_n| < n$. Ale założyliśmy przecież, że liczby M_n nie da się wygenerować programem krótszym od n. Otrzymana sprzeczność dowodzi nieobliczalności funkcji $n \mapsto P_n$. □

Uwaga. Czytelnik rozpoznał zapewne w powyższym rozumowaniu schemat paradoksu Berry'ego: M_n jest najmniejszą liczbą, której nie da się wygenerować programem krótszym od n. Ta liczba rzeczywiście istnieje, nie da się jej jednak obliczyć z n.

Podobne rozumowanie prowadzi do alternatywnego dowodu Twierdzenia Gödla o niezupełności, któremu poświęcony jest artykuł Wiktora Bartola *Eubulides, Richard, Gödel* (w tym samym numerze). Spostrzegł to Gregory Chaitin, który w tym samym czasie miał podobne idee co Kołmogorow (z tym że Kołmogorow był wtedy – w latach sześćdziesiątych XX wieku – u szczytu swojej długiej kariery, a Chaitin był jeszcze uczniem college'u). Założenia o sile wyrazu teorii są tu trochę inne, ale równie łatwe do uzyskania z prostych arytmetycznych aksjomatów.

Zakładamy mianowicie, że istnieje formuła $Kol(m, n)$ reprezentująca relację $|P_m| \leqslant n$, tzn. w teorii T dowodzi się $Kol(m, n)$, wtedy i tylko wtedy, gdy $|P_m| \leqslant n$.

Twierdzenie (Gödel–Chaitin)**.** *Jeśli teoria T spełnia powyższe założenie i jest niesprzeczna, to istnieje zdanie φ, takie że ani φ, ani $\neg\varphi$ nie są twierdzeniami T.*

Szkic dowodu. Przypuśćmy, że nie ma takiego zdania, więc w szczególności, dla każdej pary liczb m, n, w teorii T dowodzi się dokładnie jednej z formuł $Kol(m, n)$ i $\neg Kol(m, n)$. Skoro istnienie w T dowodu $Kol(m, n)$ jest równoważne $|P_m| \leqslant n$, to, wobec założonej dychotomii, istnienie w T dowodu $\neg Kol(m, n)$ jest równoważne $|P_m| > n$. Mając dane n, możemy więc, przeszukując wszystkie takie dowody, znaleźć najmniejsze M, takie że $|P_M| \geqslant n$. Podobnie jak poprzednio, nazwijmy je M_n i niech program P realizuje algorytm $x \mapsto M_x$. Jeśli w programie P podstawimy za zmienną liczbę n w postaci binarnej, to analogicznie jak poprzednio, znajdziemy (przy dostatecznie dużym n) program Q_n zaprzeczający definicji M_n. □

Inaczej niż w oryginalnym dowodzie Gödla, nie otrzymaliśmy tutaj *explicite* konstrukcji niezależnej formuły φ. Jednak argument – wywodzący się z paradoksu Berry'ego – jest chyba nieco prostszy i bardziej intuicyjny, jako że odwołuje się do tempa wzrostu funkcji w miejsce tajemniczego błędnego koła z paradoksu kłamcy. I tu, i tam widzimy, jak paradoksy, przy odpowiedniej interpretacji, stają się konstruktywnymi argumentami.