Kryptologia postkwantowa

Tomasz KAZANA

Jednym z ważniejszych osiągnięć informatyki opartej o komputer kwantowy, które zresztą eksponujemy w tym numerze *Delty*, jest opracowanie efektywnego (wielomianowego od rozmiaru danych) algorytmu na rozkład dużych liczb na czynniki pierwsze. Wspaniały, budzący zachwyt wynik. Nie dość, że przepiękny, korzystający z bardzo ładnego fragmentu matematyki, to jeszcze pozwalający wierzyć, że komputer kwantowy złożony z n kubitów jest *istotnie lepszy* od komputera klasycznego, zawierającego pamięć o n bitach. Albo inaczej: że (też prezentowany w tym numerze) model obliczeń komputera kwantowego ma istotnie większą siłę wyrazu (przy założeniu wielomianowego czasu działania) niż klasyczny model Turinga czy inne równoważne.

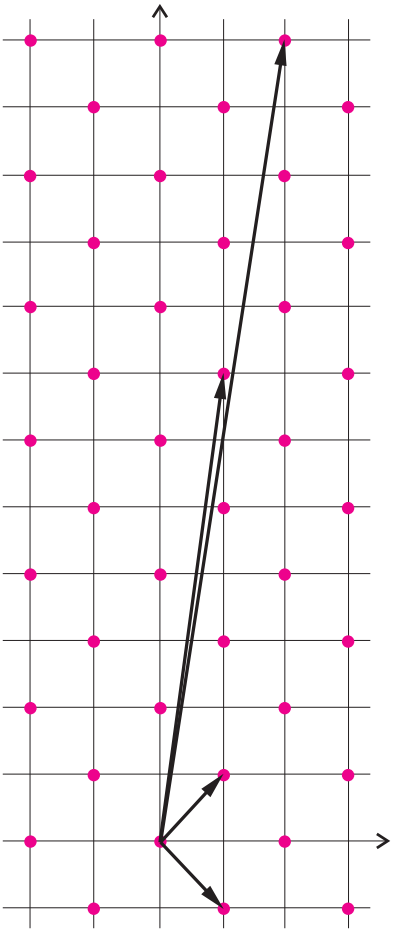
Co to znaczy w praktyce?

To znaczy, że wierzymy, iż istnieją problemy, które komputer kwantowy, mający n kubitów i wielomianowy od n czas na działanie, rozwiąże, ale już komputer klasyczny, obdarzony analogicznymi zasobami (n bitów pamięci i wielomianowy czas), im nie podoła. Hipotetycznym przykładem takiego problemu jest właśnie rozkład liczb na czynniki pierwsze. Dzięki Peterowi Shorowi wiemy, że komputer kwantowy radzi sobie z tym zadaniem. Z drugiej strony: nikt jeszcze nie potrafił pokazać, jak to zadanie rozwiązać (efektywnie) na komputerze klasycznym.

Wszystko, co powyżej, wydaje się tylko i wyłącznie zestawem dobrych wiadomości. Jednak nie do końca! W dziedzinie kryptologii istnienie lepszych niż klasyczne komputerów może powodować problemy. No bo przecież bezpieczeństwo większości protokołów kryptologicznych opiera się na założeniu, że jakiś problem jest bardzo trudny. Gdy nagle dostajemy nowe potężne narzędzie, może się przecież okazać, że pewne problemy nagle stają się już łatwe! Nie jest to wcale czcze gadanie, co od razu pokazuje algorytm Shora: przecież szyfrowanie RSA opiera się na trudności faktoryzacji, więc nie będzie ono miało sensu w świecie postkwantowym.

Kryptolodzy stoją więc przed konkretnym wyzwaniem. Chcąc przygotować świat na nadejście komputerów kwantowych, muszą projektować protokoły oparte na trudności problemów innych niż rozkład na czynniki pierwsze. Takie inne założenia w świecie kryptologów oczywiście istnieją: często zakładamy chociażby trudność problemu logarytmu dyskretnego (np. w protokole Diffiego–Hellmana), czy problemu logarytmu w grupie krzywych eliptycznych (np. w podpisie cyfrowym ECDSA). Niestety! Oba te założenia również potrafimy rozwiązywać efektywnie za pomocą (hipotetycznego) komputera kwantowego...

Dziedzina kryptologii postkwantowej rozwija się naprawdę prężnie. Na wszystkich czołowych konferencjach kryptologicznych (CRYPTO, EUROCRYPT, TCC) zawsze co najmniej jedna sesja jest ostatnio przeznaczana na ten temat. Co więcej, w roku 2006 po raz pierwszy odbyła się – i odbywa rokrocznie do dziś – konferencja PQCrypto, dedykowana wyłącznie tematyce postkwantowej w kryptologii.



Czytelnik Pełen Obaw zapewne w tym miejscu zastanawia się, czy może nie jest przypadkiem tak, że po prostu komputer kwantowy zaatakuje skutecznie *wszystkie* potencjalne protokoły kryptologiczne, bo, na przykład, będzie potrafił rozwiązać szybko każdy problem z klasy NP. Większość badaczy nie jest jednak aż tak pesymistyczna w tym temacie. To znaczy, o ile wierzy się, że komputer kwantowy *jest* lepszy od klasycznego, to jednak intuicja informatyków powszechnie skłania ich ku hipotezie, że nie jest on w stanie szybko rozwiązywać problemów NP-zupełnych.

Powyższy pogląd daje nadzieję na bezpieczną kryptologię postkwantową. Co więcej, mamy już kandydatów na problemy, które *wydają* się trudne dla komputera kwantowego. Mamy także gotowy dość szeroki wachlarz konkretnych protokołów opartych na tych założeniach. Przykładów takich protokołów tutaj podawać tym razem nie będziemy, ale chcemy przynajmniej zaprezentować problem, który przyjmujemy jako trudny w świecie postkwantowym. (Co oznacza, że badacze tej dziedziny starają się redukować do niego inne protokoły.) Opowiemy o problemie najmniejszego wektora w kracie (*shortest vector problem*, w skrócie SVP).

Załóżmy, że mamy dane n wektorów $v_i \in \mathbb{Z}^k$. Kratą całkowitoliczbową rozpiętą przez te wektory nazywamy zbiór

$$B = \left\{ u \in \mathbb{Z}^k : u = \sum_{i=1}^{n} x_i v_i \text{ dla pewnych } x_i \in \mathbb{Z} \right\}.$$

Pytamy teraz o najkrótszy (w sensie zwykłej metryki euklidesowej) niezerowy wektor w zbiorze B.

Powyższy problem (oczywiście dla odpowiednio dobranych parametrów n i k oraz umiejętnie wylosowanych wektorów v_i) uchodzi za bardzo trudny nawet dla komputera kwantowego.

Popatrzmy jeszcze przez chwilę na bardzo małe instancje problemu SVP. Proponuję dwie zagadki. Najpierw zerknijmy na zestaw: $v_1' = (1,1)$, $v_2' = (1,-1)$, a następnie na: $v_1'' = (1,7)$, $v_2'' = (2,12)$.

Pytamy, oczywiście, o najmniejszy niezerowy wektor w kratach rozpiętych przez te zestawy wektorów.

W pierwszym przypadku dość łatwo zauważyć (i udowodnić), że najmniejszymi wektorami (poza dwoma innymi, symetrycznymi względem zera) są właśnie wejściowe v_1' i v_2'. Co ciekawe, w drugiej zagadce, mimo że wejściowe wektory wyglądają groźniej, to rozpinana przez nie krata jest dokładnie tą samą kratą (czemu?), więc najmniejsze wektory to ponownie $(1,1),(1,-1),(-1,-1)$ oraz $(-1,1)$.

Podane przykłady mają na celu ilustrację jeszcze jednej własności problemu SVP. Otóż dla ustalonej kraty istnieją różne zestawy wektorów ją definiujące (tzw. bazy), co więcej: problem SVP dla różnych baz tej samej kraty może być istotnie trudniejszy. Czytelnik Domyślny, któremu kojarzy się to z kryptografią opartą o klucze prywatne i publiczne, nie myli się.

PS. Czytelnik-Profan może być z kolei zaniepokojony nadużywaniem w tym tekście zwrotów takich jak *wydaje się*, *pozwalający wierzyć* itp. Nie jest to jednak przypadek, a o tym, że kryptologia to nauka dla ludzi dużej wiary, próbowałem przekonać Czytelników już w numerze 10/2017 *Delty*.

Czytelnikowi Sumiennemu proponujemy znalezienie takich liczb całkowitych p_1 i p_2 oraz q_1 i q_2, aby było

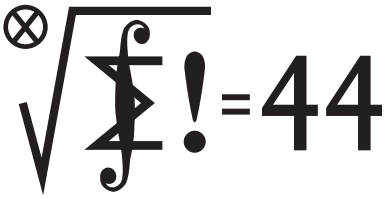
$$p_1 v_1'' + p_2 v_2'' = v_1'$$

i

$$q_1 v_1'' + q_2 v_2'' = v_2'.$$

Odpowiedź zamieściliśmy w numerze.

Klub 44

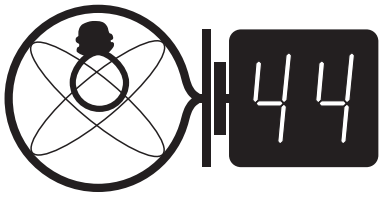


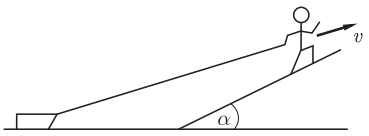
Termin nadsyłania rozwiązań: 28 II 2018

Czołówka ligi zadaniowej **Klub 44 M** po uwzględnieniu ocen rozwiązań zadań 741 ($WT = 1{,}82$) i 742 ($WT = 1{,}55$) z numeru 5/2017

Jerzy Cisło	Wrocław	47,31
Janusz Olszewski	Warszawa	46,79
Marcin Małogrosz	Warszawa	44,23
Adam Dzedzej	Gdańsk	43,22
Marcin Kasperski	Warszawa	42,59
Patryk Jaśniewski	Gdańsk	42,49
Roksana Słowik	Knurów	41,91
Franciszek S. Sikorski	Warszawa	39,71
Krzysztof Maziarz	Kraków	37,45

Widywaliśmy już te nazwiska – prawda?
Jerzy Cisło – po raz trzynasty.
Janusz Olszewski – po raz osiemnasty.
Marcin Małogrosz – po raz drugi.





Liga zadaniowa Wydziału Matematyki, Informatyki i Mechaniki, Wydziału Fizyki Uniwersytetu Warszawskiego i Redakcji *Delty*

Skrót regulaminu

Każdy może nadsyłać rozwiązania zadań z numeru n w terminie do końca miesiąca $n+2$. Szkice rozwiązań zamieszczamy w numerze $n+4$. Można nadsyłać rozwiązania czterech, trzech, dwóch lub jednego zadania (każde na oddzielnej kartce), można to robić co miesiąc lub z dowolnymi przerwami. Rozwiązania zadań z matematyki i z fizyki należy przesyłać w oddzielnych kopertach, umieszczając na kopercie dopisek: **Klub 44 M** lub **Klub 44 F**. Oceniamy zadania w skali od 0 do 1 z dokładnością do 0,1. Ocenę mnożymy przez współczynnik trudności danego zadania: $WT = 4 - 3S/N$, gdzie S oznacza sumę ocen za rozwiązania tego zadania, a N – liczbę osób, które nadesłały rozwiązanie choćby jednego zadania z danego numeru w danej konkurencji (**M** lub **F**) – i tyle punktów otrzymuje nadsyłający. Po zgromadzeniu **44** punktów, w dowolnym czasie i w którejkolwiek z dwóch konkurencji (**M** lub **F**), zostaje on członkiem **Klubu 44**, a nadwyżka punktów jest zaliczana do ponownego udziału. Trzykrotne członkostwo – to tytuł **Weterana.** Szczegółowy regulamin został wydrukowany w numerze 2/2002 oraz znajduje się na stronie `deltami.edu.pl`

Zadania z matematyki nr 751, 752

Redaguje Marcin E. KUCZMA

751. Trójkąt równoboczny o boku długości n został podzielony (prostymi równoległymi do boków) na n^2 trójkątów o boku 1 (trójkątów jednostkowych). Wierzchołkom powstałej siatki zostały przyporządkowane różne liczby rzeczywiste ($(n+1)(n+2)/2$ różnych liczb). Trójkąt jednostkowy nazwiemy zorientowanym dodatnio, jeśli – idąc wzdłuż jego brzegu, w kierunku wzrastania liczb przy wierzchołkach (tj. startując od najmniejszej i idąc przez średnią do największej) – mamy jego wnętrze po lewej stronie. Dla ustalonej liczby naturalnej n wyznaczyć najmniejszą i największą możliwą wartość liczby trójkątów jednostkowych zorientowanych dodatnio.

752. Znaleźć wszystkie pary liczb całkowitych dodatnich, których średnia arytmetyczna i średnia geometryczna różnią się o 1.

Zadanie 752 zaproponował pan Witold Bednarek z Łodzi.

Zadania z fizyki nr 648, 649

Redaguje Elżbieta ZAWISTOWSKA

648. Człowiek wchodzi ze stałą prędkością v na zbocze nachylone pod kątem α do poziomu (rysunek) i ciągnie sanki o masie m za pomocą nierozciągliwej, lekkiej linki o długości l. Sanki ślizgają się bez tarcia po powierzchni poziomej. Jakie jest naprężenie linki, gdy tworzy ona z poziomem kąt α?

649. Na bardzo cienką przezroczystą płytkę naniesiono nieprzezroczyste, koncentryczne pierścienie. Położenia i rozmiary pierścieni są tak dobrane, że równoległa wiązka światła o długości fali $\lambda = 500$ nm, padająca prostopadle na płytkę, ogniskuje się w odległości $f = 25$ cm od płytki. Rozmiary płytki są małe w porównaniu z odległością f.
a) Wyznaczyć promienie wewnętrzne i zewnętrzne dwóch najbliższych centrum nieprzezroczystych pierścieni.
b) W jakiej odległości od płytki powstanie obraz punktowego źródła światła monochromatycznego o tej samej długości fali co wiązka równoległa, umieszczonego w odległości a od płytki na jej osi przechodzącej przez środki pierścieni?