Zastosowania metod kombinatoryki addytywnej do wybranych zagadnień multiplikatywnych

Rafał Bystrzycki

Głównym celem pracy jest badanie różnych sposobów, w jakie kombinatoryka addytywna może być wykorzystana do radzenia sobie z pewnymi zagadnieniami pojawiającymi się w multiplikatywnej teorii liczb. Konkretne problemy badane przez nas dotyczą złożoności obliczeniowej obliczania wartości funkcji teorioliczbowych, sum dylatacji i sum eksponencjalnych.

Najważniejsza część pracy dotyczy następującego problemu: Przypuśćmy, że dla pewnej liczby naturalnej n i pewnej liczby pierwszej p jest nam dany zbiór reszt modulo p wszystkich dzielników liczby n i chcielibyśmy stwierdzić, które z nich odpowiadają jej czynnikom pierwszym. Przedstawiony jest algorytm rozwiązujący ten problem dla p i n spełniających pewne naturalne warunki i zostaje pokazane, że jest wiele takich liczb. Interesującą cechą przedstawionego dowodu jest to, że wymaga on użycia kombinatoryki addytywnej. Proponowany algorytm składa się z dwóch algorytmów, które wykonane jedna po drugiej prowadzą do rozwiązania. Niepowodzenie pierwszego z nich wskazuje na istnienie strukturalnych własności zbioru przekładających się na jego energię addytywną. które mogą być następnie wykorzystane w drugiej bardziej skomplikowanej części algorytmu opartej na technikach analizy fourierowskiej.

Główne twierdzenie w tej części mówi, że dla bezkwadratowej liczby całkowitej n spełniającej pewne ograniczenia i liczby pierwszej spełniającej pewne inne techniczne warunki jeśli znamy zbiór reszt modulo p wszystkich dzielników n (oznaczamy ten zbiór A_p), to istnieje efektywny deterministyczny algorytm zwracający zbiór B taki, że $\Gamma_p \subset B \subset A_p$ (gdzie Γ_p oznacza zbiór reszt modulo p czynników pierwszych liczby n) oraz $|B| < \epsilon |A_p|$

Wszystkie warunki pojawiające się w założeniach twierdzenia są bardzo słabe i tak naprawdę zachodzą dla prawie każdej liczby bezkwadratowej n oraz wystarczająco wielu liczb pierwszych p, aby możliwe było jego praktyczne zastosowanie. Pokazujemy również zastosowanie tego wyniku do algorytmu, który znajduje rozkład na czynniki danej liczby przy użyciu wyroczni na wartości funkcji $\sigma_k(n)$. Właśnie poszukiwanie deterministycznych redukcji faktoryzacji do innych problemów teorioliczbowych stanowiło oryginalną motywację do badania tego zagadnienia.

W kolejnej części pracy badany jest problem dotyczący sum eksponencjal-

nych. Dokładniej, następujące wyrażenie

$$s(a/q) = \sum_{r=1}^{\tau} e(\frac{a2^r}{q}),$$

gdzie $e(x) := \exp(2\pi i x)$ i τ jest multiplikatywnym rzędem elementu grupy odpowiadającego liczbie 2, jest rozważane. Oszacowana jest jego wartość bezwzględna. Wynik osiągnięty przez nas w tej kwestii jest następujący. Podajemy górne oszacowanie z lepszą stałą niż dotychczas znana (podana przez Kaczorowskiego i Molteniego) oraz dostarczamy nowych przykładów sytuacji, w których oszacowanie jest bliskie realizacji.

W ostatniej części pracy rozważane są oszacowania na wielkość zbioru sum dylatacji. Zbiory sum dylatacji to zbiory postaci

$$\lambda_1 \cdot A + \cdots + \lambda_h \cdot A,$$

gdzie dla dowolnego skalara λ i dowolnych zbiorów liczb całkowitych A, B przyjmujemy notację $\lambda \cdot A = \{\lambda a : a \in A\}$ oraz $A + B = \{a + b : a \in A, b \in B\}$. Seria wyników dających oszacowania górne wielkości tego zbioru jest udowodniona przy założeniu małego podwojenia, czyli dla A spełniającego $|A + A| < K|A|$ dla pewnej stałej K.

Najogólniejsze oszacowanie osiągnięte przez nas jest postaci $K^{O\left(\frac{rh}{\log(h)} + h\log(h)\right)}|A|$, gdzie r oznacza maksymalną liczbę bitów w zapisie współczynników λ_i, natomiast h jest liczbą sumowanych składników. Ten wynik stanowi wzmocnienie wyniku Bukha.

Nasze następne twierdzenie stosuje się do przypadku, gdy K jest znacznie mniejsze niż h. Pokazuje ono, że zależność od h staje się przy takich założeniach wielomianowa. Stanowi wzmocnienie poprzedniego twierdzenia w takich wypadkach.

Ostatnie twierdzenie dotyczy sytuacji gdy Λ - zbiór współczynników λ_i - ma pewną strukturę addytywną. W tym wypadku spektakularne wzmocnienie oszacowania jest możliwe. Jeśli oznaczymy przez L stałą podwojenia zbioru Λ, to oszacowanie przyjmuje postać $K^{O((h+r)L\log L)}|A|$.

Rafał Bystrzycki