Warszawa dn. 12-06-2019

Prof. UW Jacek Pomykała
Instytut Matematyki Wydział Matematyki
Informatyki i Mechaniki Uniwersytetu Warszawskiego

Recenzja rozprawy doktorskiej mgra Rafała Bystrzyckiego nt. **Applications of additive combinatorics methods to some multiplicative problems**

Rozprawa magistra Rafała Bystrzckiego jest napisana w języku angielskim i liczy 42 strony. Dotyczy zastosowania metod kombinatoryki addytywnej do wybranych zagadnień multyplikatywnych teorii liczb. Składa się z 3 rozdziałów. W pierwszym autor bada zastosowanie metod kombinatoryki addytywnej i analitycznej teorii liczb do warunkowej faktoryzacji liczb naturalnych i jest przykładem problemu faktoryzacji liczby naturalnej n z użyciem wyroczni, która zwraca wartości funkcji sumy dzielnikow $\sigma_k(n)$. Drugi dotyczy oszacowań sum wykładniczych na podgrupie generowanej przez liczbę 2, natomiast trzeci ogólnych sum dylatacji postaci

$$\lambda_1 \cdot A + ... + \lambda_h \cdot A$$

dla podzbiorów$A \subset Z$, $|\lambda_i| \leq 2^r$ i ich górnych oszacowań w zależności od wartości r oraz h.

We wszystkich rozdziałach autor wnosi istotny przyczynek w zakresie nowych zastosowań metod kombinatoryki addytywnej lub też rozszerzenia, ewentualnie wzmocnienia wyników już istniejących. Zacznę od objętościowo skromniejszych rozdziałów drugiego i trzeciego. W rozdziale drugim doktorant analizuje problem oscylacji sum wykładniczych postaci

$$s(a/q) = \sum_{r \leq \tau} e\left(\frac{a2^r}{q}\right)$$

gdzie $e(x) := e^{2\pi i.x}$ oraz τ jest rzędem multyplikatywnym dwójki modulo q.

Tutaj autor rozprawy mocno inspiruje się metodą zastosowaną w pracy Kaczorowskiego i Molteni'ego i udaje mu się porawić stałą c w ich oszacowaniu górnym postaci

$$\max_{(a,q)=1} |s(a/q)| \leq \tau - c(\kappa + 1)$$

dla $\tau \geq \kappa(\lfloor \log_2(q) + 1 \rfloor) + 2$, przy pewnej stałej dodatniej κ -Twierdzenie 2.0.4 i jej dalsze ulepszenie w Twierdzeniu 2.2.1, przy nieznacznej modyfikacji nierówności dla τ.

W rozdziale trzecim autor dowodzi górnych oszacowań dla sum dylatacji

$$\lambda_1 \cdot A + ... + \lambda_h \cdot A$$

gdzie $A \subset Z$, $|\lambda_i| \leq 2^r$ w zależności od ograniczenia na stałą podwojenia (ang. doubling constant) K dla zbioru A - Twierdzenie 3.2.1 oraz w przypadku gdy $h \geq K$ - Twierdzenie 3.2.2. Jeśli dodatkowo ciągi współczynników $\Lambda = (\lambda_i)$ posiadają pewną strukturę addytywną (stała podwojenia dla zbioru Λ jest L) to dla $\Lambda \subset [2^r]$ ostatnie oszacowanie górne autor wzmacnia do rzędu wielkości

$$K^{((h+r)L \log L)}|A|.$$

Te rezultaty poprawiają lub rozszerzają niedawne oszacowania górne otrzymane przez Schoena i Skhredova. Reasumując wyniki otrzymane przez mgra Bystrzyckiego w tym rozdziale dowodzą bardzo dobrego warsztatu i dużych umiejętności autora w tej dziedzinie.

Pierwszy rozdział jest też historycznie pierwszym tematem jaki doktorant badał w ramach swojej pracy naukowej i był motywowany problemem faktoryzacji liczb naturalych z zadaną wyrocznią. Ta problematyka ma swoje źródło w problemie redukcji faktoryzacji do obliczania wartości funkcji multyplikatywnych, gdzie najbardziej znane przykłady są związane z rzędem grupy jedności pierścienia Z_n czy krzywej eliptycznej nad pierścieniem Z_n. Autor rozprawy zastosował tu nowe podejście używając metod kombinatoryki addytywnej i analitycznej teorii liczb. W tym przypadku redukcja dotyczy wyroczni odpowiadającej wartością sumy k-tych potęg dzielników naturalnych zadanej liczby naturalnej n.

Myśl przewodnia jest następująca: Autor zakłada, znajomość odpowiednich wartości funkcji Newtona $p_k(x_1, ..., x_m) = \sum_{i=1}^{m} x_i^k$, gdzie $x_i \in \{d_1, ..., d_{\tau(n)}\}$ przebiegają wszystkie dzielniki naturalne liczby n. Korzystając z tożsamości Newtona i wzorów Viete'a oblicza współczynniki wielomianu W_p, którego pierwiastkami są wartości $d_1, ..., d_{\tau(n)} \mod p$. Następnie przy pomocy algorytmu Shoup'a faktoryzuje wielomian W_p i stosuje kluczowe algorytmy 1.2.2

oraz 1.2.7 do znalezienia odpowiedniego zbioru B spełniającego warunek

$$\Gamma_p \subset B \subset A_p$$

gdzie $|B| < \varepsilon |A_p|$, Γ_p jest zbiorem redukcji mod p dzielników pierwszych n, natomiast A_p zbiorem redukcji mod p wszystkich dzielników $d_1, ..., d_{\tau(n)}$.

To pozwala (stosując podniesienie Hensela) na efektywne znalezienie wszystkich dzielników pierwszych n w kroku 6 algorytmu 1.5.1. Kluczowym elementem dowodu jest wykazanie, że algorytmy 1.2.2 oraz 1.2.7 dopełniają sięwzajemnie dla "generycznej" liczby naturalnej n. W drugim z nich jest w wyrafinowany sposób wykorzystana struktura addytywna obrazu homomorficznego zbioru A_p przy zastosowaniu wartości logarytmów dyskretnych modulo p. To jest miejsce gdzie autor wplata bogaty warsztat kombinatoryki addytywnej do osiągnięcia postawionego przed sobą celu. Drugim ważnym elementem jest problem "generyczności" liczby n, dla której odpowiedni zbiór posiada pewną strukturę addytywną. Autor dojrzale wykorzystuje tu narzędzia analitycznej teorii liczb. Z jednej strony stosując Twierdzenie Bombieriego-Vinogradova pokazuje, że wystarczająco dużo jest liczb pierwszych p dla, których największy dzielnik pierwszy $p-1$ ma epsilonową lokalizację w otoczeniu wartości $p^{1/2}$. Z drugiej strony, że odpowiednio mało jest liczb naturalnych $n \leq x$, dzielących się przez kwadrat liczby całkowitej większej niż $\log\log x$. Ponadto doktorant dowodzi istotnego oszacowania pokazującego, że dla prawie wszystkich n zbiór dzielników naturalnych $d \mid n$ liczby n spełniających warunek

$$d^{(p-1)/P(p-1)} \equiv q^{(p-1)/P(p-1)} \mod p$$

dla pewnego dzielnika pierwszego $q > p$ liczby n jest odpowiednio mały. Tu $P(a)$ oznacza największy dzielnik pierwszy a. Z obliczeniowego punktu widzenia istotnym jest wykazanie, że krok czwarty algorytmu 1.2.7 ma niewielką złożoniość obliczeniową. Te cząstkowe wyniki sumarycznie prowadzą do konkluzji, że metoda pozwala sfaktoryzować (przy użyciu proponowanej wyroczni) prawie wszystkie liczby naturalne n w bardzo dobrym czasie deterministycznym $O((\log n)^{1+2\log 2+o(1)})$, gdy n dąży do nieskończoności.

Rozprawa jest generalnie dobrze zredagowana choć gdzieniegdzie zdarzają się literówki, np. nazwisko Schwarz na stronie 10 jest napisane błędnie, w terści Twierdzenia 0.0.9 brak jest oznaczenia zbioru A, natomiast w definicji 0.0.15 powinno być $g \in G$. Brakuje mi trochę precyzji w sformułowaniach algorytmów (co utrudnia lekturę pracy) - np. moim zdaniem w pierwszym akapicie algorytmu powinny być dokładnie podawane jego dane wejściowe i wyjściowe.

Merytorycznie praca jest bardzo dobra, a udowodnione rezultaty wplatają się w badania prowadzone przez innych znaczących matematyków w świecie. Całość rozprawy jest spójna ze względu na metody stosowe do wykazania postulowanych rezultatów. Ponadto jest solidnie podbudowana trzema publikacjami autora. Reasumując uważam, wkład doktoranta za znaczący i przyczyniający się do dalszego rozwoju zastosowań metod kombinatoryki addytywnej w dziedzinie teorii liczb i kryptologii. Uważam, że rozprawa przedstawia oryginalne rozwiązanie problemu naukowego oraz dowodzi ogólnej wiedzy teoretycznej doktoranta w tej dziedzinie. Mimo pewnych usterek (głównie natury językowej), praca jest dobrze zredagowana a jej poziom naukowy jest bardzo wysoki.

Konkludując uważam, że rozprawa mgr Rafała Bystrzyckiego nt. *Applications of additive combinatorics methods to some multiplicative problems* spełnia wymagania artykułu 13.1 Ustawy o stopniach naukowych i tytule naukowym z dn. 14 marca 2003 roku. Może być zatem podstawą do nadania magistrowi Rafałowi Bystrzyckiemu stopnia naukowego doktora w dziedzinie nauk matematycznych, w dyscyplinie matematyka. W związku z powyższym przedkładam Radzie Naukowej Wydziału Matematyki i Informatyki UAM wniosek o przyjęcie tej rozprawy i dopuszczenie mgra Rafała Bystrzyckiego do dalszych etapów przewodu doktorskiego.

Jacek Pomykała