dr hab. prof. US Andrzej Dąbrowski
Instytut Matematyki
Uniwersytet Szczeciński

Szczecin, 23 kwietnia 2019

Recenzja rozprawy doktorskiej mgra Rafała Bystrzyckiego pod tytułem "Applications of additive combinatorics methods to some multiplicative problems"

Rozprawa doktorska mgra Rafała Bystrzyckiego dotyczy matematyki dyskretnej. Jej celem jest zastosowanie metod kombinatorycznych do pewnych zagadnień multyplikatywnej teorii liczb. Problemy te dotyczą złożoności obliczeniowej wyznaczania wartości funkcji teorioliczbowych, sum wykładniczych i sum dylatacji.

Rozprawa doktorska Pana Bystrzyckiego składa się ze wstępu oraz trzech rozdziałów. Każdy z rozdziałów odpowiada zawartości jednego z następujących trzech artykułów (w tej samej kolejności):

1. *Detection of primes in the set of residues of divisors of a given number*, Number-Theoretic Methods in Cryptology, LNCS **10737** (2018), 178-194

2. *Exponential sums over subgroups generated by* 2, Integers: Electronic Journal of Combinatorial Number Theory **18** (2018), #A24

3. *Alternative approach to sums of dilates*, Notes on Number Theory and Discrete Mathematics **24** (2018) [współautor: T. Schoen]

W pracy [1] autor rozważa następujące zagadnienie:

Załóżmy, że dla pewnej liczby naturalnej n i pewnej liczby pierwszej p znamy zbiór reszt względem modułu p wszystkich dzielników liczby n. Chcemy stwierdzić, które z nich odpowiadają jej czynnikom pierwszym.

Autor podaje algorytm rozwiązujący powyższy problem dla par $(n.p)$ spełniających pewne warunki. Sformułowanie algorytmu (Theorem 1.0.6) jest dość techniczne. Należy podkreślić, że założenia twierdzenia 1.0.6 (warunki

przy których algorytm działa) są bardzo słabe i zachodzą dla prawie każdej liczby bezkwadratowej n oraz dostatecznie wielu liczb pierwszych p. Jest to istotne w kontekście zastosowań praktycznych.

Autor podaje zastosowanie swoich wyników do algorytmu znajdującego rozkład na czynniki danej liczby przy użyciu wyroczni na wartości funkcji $\sigma_k(n)$.

W pracy [2] autor uogólnił główny wynik z artykułu J. Kaczorowskiego i G. Molteniego [*External values for the sum* $\sum_{r=1}^{\tau} e(a2^r/q)$, J. Number Theory **132** (2012), 2595-2603]. Niech τ oznacza rząd 2 w grupie $\mathbb{Z}_q^\times$, $s(a/q) := \sum_{r=1}^{\tau} \exp(2^{r+1}a\pi i/q)$ oraz $\mathcal{L} = |\log_2(q)|$. Kaczorowski i Molteni udowodnili, że dla dowolnej liczby całkowitej nieujemnej κ oraz liczby naturalnej $q > 3$, jeśli $\tau > \kappa(\mathcal{L}+1)+2$, to $\max_{(a,q)=1} |s(a/q)| < \tau - \kappa - 1$. Autor rozprawy polepsza powyższy rezultat, dowodząc, że dla dowolnej liczby dodatniej κ, $q > 3$ oraz $\tau > \kappa(\mathcal{L}+4)+5$ zachodzi nierówność $\max_{(a,q)=1} |s(a/q)| < \tau - 2(\kappa+1)$. Polepszenie stałej w nierównośći uzyskanej przez Kaczorowskiego i Molteniego jest przy założeniu wzrostu τ. Metody dowodowe wykorzystują idee pracy Kaczorowskiego i Molteniego. Autor rozważa dalsze polepszenie rezultatu, dowodząc w szczególności, że stałą 2 można zastąpić przez 2,37, jeśli tylko $\tau > \kappa(\mathcal{L}+5)+6$.

W pracy [3] autorzy rozważają oszacowania na wielkość zbioru sum dylatacji. , tj. zbiorów postaci $\lambda_1 A + ... + \lambda_h A$. Autorzy uzyskują górne oszacowania przy założeniu małego podwojenia, tj. dla A spełniającego $|A+A| < KA$ dla pewnej stałej K. Autorzy uzyskują ładne wzmocnienie rezultatu B. Bukha [*Sums of dilates*, Combin. Probab. Comput. **17** (2008), 627-639]: jest ono postaci $K^{O(\frac{rh}{\log(h)}+h\log(h))}|A|$, gdzie r oznacza maksymalną liczbę bitów w zapisie współczynników λ_i. Jest to treścią twierdzenia 3.2.1.

Następny rezultat (twierdzenie 3.2.2) stosuje się do przypadku, gdy K jest znacznie mniejsze od h. W tym przypadku zależność od h staje się wielomianowa. Jest to wzmocnienie rezultatu T. Schoena i I. D. Shkredova [*Additive dimension and a theorem of Sanders*, J. Australian Math. Soc. **100** (2016), 124-144].

Ostatni rezultat trzeciego rozdziału (twierdzenie 3.2.3) dotyczy sytuacji, gdy zbiór $\Lambda = \{\lambda_1, ..., \lambda_h\}$ ma pewną strukturę addytywną. W tym przypadku oszacowanie przyjmuje postać $K^{O((h+r)l\log L)}|A|$, gdzie L oznacza stałą podwojenia zbioru Λ.

W rozprawie znalazłem sporo drobnych błędów i nieścisłości, które można dość łatwo poprawić (np. wystarczyło przejrzeć tekst przez wysłaniem do recenzentów). Oto większość z nich:

– autor często pomija słowo *finite* (patrz, np. Lemma 0.0.8, Definition 0.0.2, Theorem 0.0.9, Lemma 0.0.17, Lemma 1.2.3, Lemma 1.3.2, Theorem 3.0.1, Corollary 3.1.4, ...

– druga część Definicji 0.0.15 nie jest precyzyjna (czym jest $v \cdot [M, N]$?); podobna uwaga dotyczy definicji 0.0.16.

– strona 14, Preliminaries: powinno być "in sections 1.3 and 1.4"

– Lemma 1.1.7: Assume p is an odd prime.

– (1), (2), (3), (4) w Introduction powinny być oznaczane przez (0.1), ...

– sformułowanie Theorem 1.3.4 nie jest poprawne

– Definition 1.3.7: co oznacza zapis $K \subset a, a + d, ..., a + ld$?

– str. 32, przed 2.2: the proof of Theorem 2.0.3

– str. 36, linia 10-: Proposition 0.0.14

Najwięcej nieścisłości zawierają wstęp oraz rozdział pierwszy, co trochę utrudnia lekturę tej części rozprawy. Rozdziały 2 i 3 są napisane dużo lepiej.

Osiągnięcia naukowe mgra Rafała Bystrzyckiego uzyskane w rozprawie oceniam pozytywnie. Pierwsze moje wrażenie było takie, że praca jest zbyt elementarna aby mogła spełniać wymogi rozprawy doktorskiej. Bardziej wnikliwa lektura tej pracy przekonała mnie, że jest to wartościowa rozprawa (mimo że dość elementarna) z ciekawymi zastosowaniami.

Rezultaty uzyskane w rozprawie są wartościowe. Dowody nie są zbyt skomplikowane technicznie, jednak rozumowania są dość pomysłowe. Autor wykazał się znajomością aktualnej literatury oraz biegłym opanowaniem pewnych technik z zakresu kombinatoryki, analitycznej teorii liczb i złożoności obliczeniowej. Wszystkie rezultaty rozprawy zostały opublikowane przed jej obroną, co nie jest częstym zjawiskiem.

W moim przekonaniu (pomimo zastrzeżeń dotyczących redakcji) rozprawa mgra Rafała Bystrzyckiego spełnia ustawowe i zwyczajowe wymogi stawiane rozprawom doktorskim. Wnoszę o dopuszczenie jej do dalszych etapów przewodu doktorskiego.

A. Dąbrowski