STRESZCZENIE ROZPRAWY DOKTORSKIEJ PT. ADDITIVE PROBLEMS IN ABELIAN GROUPS

KAROL CWALINA

Rozprawa prezentuje kilka wyników dotyczących addytywnych właściwości skończonych zbiorów w grupach przemiennych. Obiektem naszego szczególnego zainteresowania będą zwłaszcza zbiory sum (ang. *sumsets*) określone dla podzbiorów A, B dowolnej grupy przemiennej jako $A + B = \{a + b : a \in A, b \in B\}$.

Rozważane zagadnienia są dwojakiego rodzaju. Jedne stanowią rodzaj strukturalnej teorii arytmetyki zbiorów i za cel stawiają sobie możliwie dokładną charakteryzację zbiorów określonych poprzez pewne ekstremalne własności. W naszym wypadku będą to zbiory o niewielkim współczynniku podwojenia (ang. *doubling*), który jest zdefiniowany dla dowolnego skończonego podzbioru A grupy przemiennej jako $K(A) = |A + A|/|A|$. W związku z tym zagadnieniem badamy twierdzenie Greena-Ruzsy, które niemal całkowicie charakteryzuje zbiory o niewielkim współczynniku podwojenia. W szczególności, dowodzimy pierwszego liniowego ograniczenia na wymiar ciągu w tym twierdzeniu.

Drugim obszarem naszego zainteresowania jest analiza równań liniowych w grupach przemiennych, a celem określenie warunków istnienia (nietrywialnych) rozwiązań tych równań lub oszacowanie liczby tych rozwiązań. Dla porządku zauważmy, że zagadnienia te są równoważne problemom istnienia, oraz pytaniom o liczbę, nietrywialnych reprezentacji zera w zbiorach postaci $a_1 \cdot A + \cdots + a_k \cdot A$ dla zadanych całkowitych współczynników $a_1, \ldots, a_k$, gdzie $a \cdot A = \{ax : x \in A\}$. W pracy dowodzimy pierwszego wolno rosnącego górnego ograniczenia na wielkość liczb typu Ramseya związanych z ogólnymi równaniami liniowymi. Przedstawiamy również dowód hipotezy Schinzla, związanej z liczbą rozwiązań równań liniowych w grupach cyklicznych.

Zauważmy, że oba wspomniane zagadnienia pozostają ze sobą w pewnym związku. Intuicja każe spodziewać się, że współczynnik podwojenia zbioru A jest związany z liczbą rozwiązań w tym zbiorze równania $x + y = x' + y'$. Częściową odpowiedniość pomiędzy tymi wielkościami ustanawia, udowodnione w [BS94], a z pierwszymi mocnymi ograniczeniami w [Gow01, Proposition 7.3], twierdzenie Balog-Szemerédiego(-Gowersa).

1. Zbiory o niewielkim współczynniku podwojenia

Oczywiste jest, że $K(A) \leqslant \binom{|A|+1}{2}$ i bez większych trudności można skonstruować takie zbiory $A \subseteq \mathbb{Z}$, dla których zachodzi równość. Z drugiej strony, dla $A \subseteq \mathbb{Z}$ zawsze mamy $|A+A| \geqslant 2|A|-1$ i równość zachodzi tylko dla zbiorów będących ciągami arytmetycznymi. Podobnie, dla dowolnej rodziny $P_1, \dots, P_d$ ciągów arytmetycznych, w przypadku zbioru $A = P_1 + \dots + P_d$ mamy $|A+A| \leqslant 2^d|A|$. Zbiory powyższej postaci nazywamy *d-wymiarowymi uogólnionymi ciągami arytmetycznymi*. W szczególności, jeśli $d = O(1)$, wciąż możemy utrzymywać, że współczynnik podwojenia jest mały. Oczywiście każdy duży podzbiór uogólnionego ciągu arytmetycznego również ma mały współczynnik podwojenia.

Okazuje się, że powyższe zdanie stanowi pełną charakteryzację zbiorów o niewielkim współczynniku podwojenia, tzn. każdy taki zbiór A jest podzbiorem pewnego $d(K)$-wymiarowego ciągu arytmetycznego o rozmiarze niewiększym niż $f(K)|A|$. Pierwszy dowód tego twierdzenia pochodzi od Freimana [Fre73], ale uzyskane przez niego ograniczenia na funkcje d, f było dość słabe. Okres prawdziwego zainteresowania tym twierdzeniem na przełomie tysiącleci wiąże się z dwoma zdarzeniami.

Pierwszym z nich było pojawienie się nowego, bardzo ustrukturalizowanego i analitycznego w charakterze dowodu autorstwa Ruzsy [Ruz94]. Naśladując nakreślony przez Ruzsę ogólny model dowodzenia twierdzeń typu Freimana, kolejni autorzy poprawiali ograniczenia na rozmiar odpowiedniego ciągu arytmetycznego. Obecnie najlepsze wyniki pochodzą od Chang [Cha02], $d(K) = K + o(1)$ i $f(K) = \exp(O(K^2 \log^{O(1)} K))$, i Sandersa [San12] $d(K), \log f(K) = K \log^{O(1)} K$. Można przy tym pokazać, że takie ograniczenia są bliskie optymalnym.

Drugim czynnikiem pobudzającym zainteresowanie twierdzeniem Freimana było pojawienie się fundamentalnych zastosowań tego twierdzenia oraz wspomnianego twierdzenia Baloga-Szemerédiego(-Gowersa), które pokazały, jak owocne mogą być rozważania o charakterze kombinatorycznym. Chodzi o przełomowe prace [Gow98, Gow01], w których Gowers podaje nowy dowód twierdzenia Szemerédiego o ciągach arytmetycznych oraz pracę Bourgaina [Bou99], poświęconą wymiarowi zbiorów Kakei.

Twierdzenie Greena-Ruzsy. W tej sytuacji naturalne jest, by spróbować rozszerzyć zakres stosowalności twierdzenia Freimana do wszystkich grup przemiennych. Nie wystarczy jednak rozważanie niskowymiarowych uogólnionych ciągów arytmetcznych jako idealnych obiektów, w których miałyby się efektywnie zawierać zbiory o małym współczynniku podwojenia. Przekonuje nas o tym rozważenie rodziny przykładów $A = G = \mathbb{F}_2^n$, dla której odpowiedni ciąg musiałby być wymiaru $n \neq O_K(1)$. Okazuje się, że odpowiednie obiekty to *ciągi warstw*, tzn. zbiory postaci $P+H$, gdzie P jest uogólnionym ciągiem arytmetycznym, a $H \leqslant G$ podgrupą.

Pierwszy tego typu ogólny wynik uzyskali Green i Ruzsa [GR07]. Dowiedli oni, że jeśli $K(A) = K$, to $A \subseteq P + H$, gdzie P jest $d(K)$-wymiarowym uogólnionym ciągiem arytmetycznym oraz $\mathrm{size}(P)|H| \leqslant f(K)|A|$. Ograniczenia podane przez Greena i Ruzsę to $d(K), \log f(K) = K^4 \log^{O(1)} K$. Następnie wynik ten został poprawiony przez Sandersa [San12], który pokazał, że można uzyskać $d(K), \log f(K) = K \log^{O(1)} K$.

W pracy pokazujemy, że w przypadku ogólnym możliwe jest podanie liniowego ograniczenia na wymiar ciągu arytmetycznego w tezie twierdzenia Greena-Ruzsy, przy zachowaniu kontroli nad rozmiarem ciągu, podobnie jak ma to miejsce w twierdzeniu Chang dla podzbiorów $\mathbb{Z}$. Dowodzimy między innymi następującego twierdzenia.

Theorem 3.13 (wariant) Niech podzbiór $A \subseteq G$ dowolnej grupy przemiennej spełnia $|A+A| \leqslant K|A|$. Wówczas albo istnieje ciąg warstw $P+H$ taki, że $A \subseteq P+H$ oraz $\dim(P) \leqslant 2K$ i $\mathrm{size}(P)|H| \leqslant \exp(O(K^2 \log^3 2K))|A|$, albo A jest pokryty przez $O(K^3 \log^2 K)$ warstw pewnej podgrupy, o łącznym rozmiarze ograniczonym przez $\exp(O(K \log^{O(1)} 2K))|A|$.

Szkic rozumowania. Ogólna idea stojąca za przedstawionym w pracy dowodem Twierdzenia 3.13 wygląda następująco. W pierwszej kolejności stosujemy twierdzenie Greena-Ruzsy i w efekcie uzyskujemy włożenie $A \subseteq P + H$. Jeśli zrobimy to w odpowiedni sposób, możemy je traktować tak, jakby P było ciągiem w grupie beztorsyjnej i zastosować twierdzenie Chang do rzutu $\pi(A)$ zbioru A na P. Szczęśliwie, rzut $\pi(\cdot)$ jest dobrze określony jeśli tylko spełnione są te same łagodne warunki, które pozwolą nam traktować ciąg jak leżący w grupie beztorsyjnej.

Tym, co stanowi istotne novum naszej pracy jest poniższy Lemat, który wiąże ze sobą własności addytywne zbioru A oraz jego rzutu $\pi(A)$.

Lemma 3.12 (wariant) Niech $A \subseteq P+H$ dla odpowiedniego ciągu warstw $P+H$ oraz niech $K_{\min} = \min_{Y \subseteq \pi(A)} |Y + \pi(A)|/|Y|$. Wtedy $K(A) \geqslant K_{\min}$.

Co ciekawe, wcale nie musi być tak, że $K_{\min} = \Omega(K(\pi(A)))$. Z nierówności Plünnecke-Ruzsy można wprawdzie uzyskać nierówność $K_{\min} \geqslant \sqrt{K(\pi(A))}$, ale twierdzenie Chang pozwoliłoby wtedy zaledwie na otrzymanie ciągu wymiaru $d(K) = K^2 + o(1)$. Aby uporać się z tą trudnością wybieramy zbiór $Y \subseteq \pi(A)$, który minimalizuje iloraz $|Y + \pi(A)|/|Y|$, a następnie stosujemy do niego lemat pokryciowy Ruzsy.

Ta część rozprawy oparta jest na materiale opublikowanym w pracy [CS13a].

2. Nie-niezmiennicze równania liniowe

Przytoczony wcześniej przykład równania $x + y = x' + y'$ sugerował istnienie związku między analizą równań a kombinatoryką addytywną. W drugiej części rozprawy wykorzystujemy niektóre z narzędzi, jakie zostały rozwinięte w toku badań nad twierdzeniami typu Freimana, aby poprawić nasze zrozumienie równań liniowych jednorodnych[1].

Naturalnym pytaniem, jakie można by w tym kontekście zadać, jest pytanie o to jak duży powinien być zbiór $A \subseteq \{1, \dots, N\}$, aby sam rozmiar gwarantował istnienie rozwiązania zadanego równania liniowego. Zagadnienie to jest już jednak dogłębnie zbadane w klasie równań zwanych *niezmienniczymi*, tj. równań o współczynnikach sumujących się do zera, z drugiej zaś strony jest trywialne w przypadku równań które nie są niezmiennicze. Przykładowo równanie $x + y = z$ nie ma rozwiązań w zbiorze liczb nieparzystych, pomimo dużej gęstości tego zbioru. Podobnie, dla każdego nie-niezmienniczego równania liniowego, można wybrać pewną klasę reszt rozmiaru $\Theta(n)$ wolną od rozwiązań tego równania.

W związku z tym badanie równań nie-niezmienniczych przebiega nieco innym torem związanym z pytaniem o regularność równania. Równanie liniowe nazywamy *regularnym*, jeśli dla dowolnego kolorowania liczb naturalnych na skończenie wiele kolorów równanie ma monochromatyczne (nietrywialne[2]) rozwiązanie. Równoważnie mówi się też o podziale $\mathbb{N} = A_1 \cup \ldots \cup A_k$ na parami rozłączne zbiory A_i, a równanie jest regularne jeśli w którymś z A_i znajduje się (nietrywialne) rozwiązanie tego równania. Jest to zatem zagadnienie typu Ramseya. Warunek regularności jednrodnego równania liniowego został podany przez Rado [Rad33]: równanie jest regularne wtedy i tylko wtedy, gdy suma niektórych z jego współczynników wynosi zero.

Można pokazać, że dla dowolnego równania regularnego i liczby $n \in \mathbb{N}_+$ istnieje taka najmniejsza liczba typu Ramseya $\mathsf{R}(n)$, że dla dowolnego n-kolorowania zbioru $\{1, \dots, \mathsf{R}(n)\}$ istnieje monochromatyczne rozwiązanie tego równania. W drugiej częśći rozprawy stawiamy pytanie o ograniczenia na $\mathsf{R}(n)$.

Łatwo pokazać, że jeśli równanie nie jest niezmiennicze, to $\mathsf{R}(n) \geqslant C^n$, dla pewnej stałej C. Dużo jednak trudniej o dobre ograniczenia górne. Można by w tym celu naśladować metodę dowodową wykorzystaną przez Rado, jednak finitystyczne

[1] W dalszym ciągu streszczenia będziemy się posługiwali określeniem *równanie liniowe* w znaczeniu jednorodnego równania liniowego

[2] Równania niezmiennicze mają zawsze trywialne rozwiązania, w których wszystkie zmienne przyjmują tę samą wartość. Takie rozwiązania nas jednak nie satysfakcjonują.

dowody odpowiedniej implikacji polegają na zastosowaniu twierdzenia van der Waerdena, co prowadzi do oszacowania postaci $\mathsf{R}(n) \ll \mathsf{tower}(5n)$, gdzie

$$\mathsf{tower}(n) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \Big\} \text{ n razy}.$$

Główny wynik tej części pracy to następujące twierdzenie.

Theorem 5.4 Niech $a_1x_1+\cdots+a_kx_k = 0$ będzie regularnym równaniem liniowym. Wtedy dla dowolnego n mamy

$$\mathsf{R}(n) \ll 2^{O(n^4 \log^4 n)},$$

przy czym odpowienie stałe zależą od współczynników $a_1, \ldots, a_k$.

Oprócz tego twierdzenia dowodzimy też jego dwóch wariantów, w których zakładamy szczególną postać rozważanych równań.

Szkic rozumowania. Na mocy twierdzenia Rado możemy założyć, że rozważane równanie regularne jest postaci $ax - ay = bz$, gdzie a, b są względnie pierwszymi liczbami naturalymi. Niech teraz $A \subseteq \{1, \ldots, \mathsf{R}(n)\}$ będzie jednym z kolorów, a jego gęstość w $\{1, \ldots, \mathsf{R}(n)/a\}$ wynosi $\delta \geqslant \frac{1}{n}$. Można by pokazać, że w zbiorze $a\cdot A - a\cdot A$ znajduje się ciąg arytmetyczny o początku w zerze i długości przynajmniej $f(\mathsf{R}(n)/a, \delta)$. Wówczas, ponieważ $a \cdot A - a \cdot A$ jest rozłączny z $b \cdot A$, podzielne przez b elementy tego ciągu należą do pozostałych $n-1$ kolorów. Zatem $\mathsf{R}(n-1) \geqslant f(\mathsf{R}(n)/a, \frac{1}{n})/b$, skąd możemy uzyskać ograniczenie górne na $\mathsf{R}(n)$.

Rozumowanie w postaci przedstawionej powyżej jest bardzo wrażliwe na to, jak dobre oszacowania potrafimy udowodnić dla funkcji $f(\cdot,\cdot)$. Napotykamy w tym miejscu na zasadnicze trudności dwóch rodzajów.

Po pierwsze, ciągi arytmetyczne nie są najlepszymi obiektami, jakich możemy poszukiwać w zbiorach różnic, gdyż wydają się zbyt regularne z arytmetycznego punktu widzenia, by pasować do metod analizy fourierowskiej, którymi dowodzi się oszacowań dla funkcji $f(\cdot,\cdot)$, a które wyewoluowały ze wspomnianej już pracy Ruzsy [Ruz94] nad twierdzeniem Freimana. W pracy, zamiast ciągów arytmetycznych poszukujemy tzw. *zbiorów Bohra*, określonych analitycznie jako

$$B(\Gamma, \gamma) = \left\{x \in \mathbb{Z}_n : \forall_{t\in\Gamma} \left\| \frac{tx}{N} \right\| \leqslant \gamma \right\},$$

gdzie $\Gamma \subseteq \widehat{\mathbb{Z}_n} \backsimeq \mathbb{Z}_n$ oznacza pewien zbiór charakterów, a $\gamma \in (0, \frac{1}{2}]$ jest parametrem.

Po drugie, prosty zbiór różnic taki jak $A - A$ nie musi zawierać odpowiednio dużych zbiorów Bohra. Pod tym względem dużo regularniejsze okazują się iterowane zbiory różnic. Przykładowo, jeśli dla zbioru $A \subseteq \{1, \ldots, N\}$ o gęstości δ możemy się spodziewać w $A - A$ ciągu arytmetycznego rozpoczynającego się zerem o długości $\Omega(\log N / \log(1/\delta))$, to w zbiorze $2A - 2A$ już ciągu długości $\Omega(N^{1/\log^4(1/\delta)})$ i dokładnie to samo zachowanie występuje, gdy szukamy zbiorów Bohra. Jest to

źródłem komplikacji, które w przypadku równań regularnych o ogólnej postaci powodują, że dowód nie przebiega już liniowo poprzez wykluczanie kolejnych kolorów, jak to miało miejsce w zarysowanym powyżej szkicu.

Kluczem do wszystkich udowodnionych w tej części pracy twierdzeń są liczne twierdzenia i lematy o istnieniu zbiorów Bohra w różnorakich zbiorach sum i różnic, albo chociaż w ich pobliżu. Zdecydowana większość z nich pochodzi wprost lub pośrednio od Sandersa [San12], który dowiódł ich w toku prac nad tzw. wielomianową hipotezą Freimana-Ruzsy (ang. *polynomial Freiman-Ruzsa conjecture*), blisko związaną z zagadnieniami poruszanymi w pierwszej części rozprawy.

Liczby typu Schura. Z ogólnych rozważań opisanych powyżej wynika, że dla regularnych nie-niezmiennicznych równań liniowych mamy

$$C^n \leqslant \mathsf{R}(n) \leqslant \exp(O(n^4 \log^{O(1)} n)) .$$

Naturalne jest więc dążenie by jeszcze bardziej zbliżyć do siebie oba ograniczenia. Dlatego rozdział poświęcony regularnym równaniom liniowym kończymy badając szczególnie proste równania o postaci $x_1 + \ldots + x_{k+1} = y_1 + \ldots + y_k$, będące uogólnieniem równania Schura $x + y = z$.

Niech $\mathsf{S}_k(n)$ oznacza liczbę $\mathsf{R}(n)$ związaną z odpowiednim uogólnieniem równania Schura; oczywiście mamy $\mathsf{S}_1(n) \geqslant \mathsf{S}_2(n) \geqslant \ldots$. Z klasycznego argumentu Schura [Sch17] wynika, że $\mathsf{S}(n) = \mathsf{S}_1(n) \leqslant en!$. W rozprawie natomiast pokazujemy, że $\mathsf{S}_k(n) = o(n!)$ dla $k \geqslant 2$.

Aby zarysować dowód tego wyniku przypomnijmy rozumowanie Schura. Niech $X_0 = \{1, \ldots, \mathsf{S}(n) - 1\} = A_1 \cup \cdots \cup A_n$ będzie podziałem bez monochromatycznych rozwiązań równania $x + y = z$. Mając zbiór $X_{k-1} \subseteq A_k \cup \ldots \cup A_n$ taki, że $X_{k-1} - X_{k-1}$ jest rozłączny z $A_1 \cup \ldots \cup A_{k-1}$, możemy założyć, że $X_{k-1} \cap A_k$ jest najliczniejszy spośród $X_{k-1} \cap A_k, \ldots, X_{k-1} \cap A_n$. Wówczas $X_k = (X_{k-1} \cap A_k \setminus \{a\}) - a$, gdzie $a = \min X_{k-1} \cap A_k$, spełnia *mutatis mutandis* te same warunki co X_{k-1}. Iterując opisany proces, po n krokach otrzymujemy zbiór X_n rozmiaru rzędu $\mathsf{S}(n)/n!$ taki, że $(X_n - X_n) \cap \mathbb{N}_+ = \emptyset$, skąd $\mathsf{S}(n) \ll n!$.

Można sprawdzić, że jeślibyśmy w kolejnych krokach mogli założyć, że zbiór $X_{k-1} \cap A_k$ ma trochę więcej elementów niż ich oczekiwana liczba, to uzyskane ograniczenie na liczbę $\mathsf{S}(n)$ mogłoby być silniejsze. To w ogólności nie musi być prawdą, ale jeśli dodatkowo założymy, że kolorowanie $A_1, A_2, \ldots$ jest w odpowiednim sensie ekstremalne, możemy uzyskać następujący substytut wspomnianego założenia.

Lemma 5.25 (wersja dla liczb $\mathsf{S}(n)$) Jeśli $N < \mathsf{S}(n)$, to istnieje taki podział $\{1, \ldots, N\} = A_1 \cup \cdots \cup A_n$ na zbiory wolne od sum, że $|A_1| \geqslant \ldots \geqslant |A_n|$ oraz

$$\bigcup_{i>k} A_i \subseteq (A_k - A_k) \cup (A_k + A_k)$$

dla wszystkich $1 \leqslant k \leqslant n$.

O ile nie potrafimy wykorzystać tego warunku w analizie liczb $\mathsf{S}(n)$, to podobny mu związany z liczbami $\mathsf{S}_k(n)$ dla $k \geqslant 2$, w połączeniu z nierównością Plünnecke-Ruzsy, daje nam wystarczający przyrost gęstości dla zbiorów otrzymywanych w kolejnych krokach argumentu Schura.

Ta część rozprawy oparta jest na zgłoszonej do publikacji pracy [CS13b].

3. Problem Schinzla

W ostatnim rozdziale rozprawy dowodzimy hipotezy postawionej przez Schinzla [Sch08, Sch09], która traktuje o liczbie rozwiązań jednorodnych równań liniowych w grupach cyklicznych. Dokładniej, dla dodatnich liczb całkowitych n, k, ciągu współczynników $\boldsymbol{a} = (a_1, \ldots, a_k)$ oraz liczb naturalnych $\boldsymbol{b} = (b_1, \ldots, b_k)$ pytamy o liczbę rozwiązań kongruencji

$$a_1x_1 + \cdots + a_kx_k \equiv 0 \pmod{n}$$

w liczbach całkowitych $x_1, \ldots, x_k$ spełniających warunek $0 \leqslant x_i \leqslant b_i$ i oznaczamy tę liczbę przez $N_n(\boldsymbol{a}, \boldsymbol{b})$.

Dowiedziona przez nas hipoteza ma następującą postać.

Theorem 6.1 Przy powyższych oznaczeniach mamy

$$N_n(\boldsymbol{a}, \boldsymbol{b}) \geqslant 2^{1-n} \prod_{i=1}^{k} (1 + b_i)\,.$$

Kluczowe jest przy tym, że czynnik 2^{1-n} nie zależy od żadnego z paramterów poza n. Rozważając to zagadnienie dla $a_i = b_i = 1$, w przypadku $k = n - 1$, widzimy, że $N_n(\boldsymbol{a}, \boldsymbol{b}) = N_n(\mathbf{1}, \mathbf{1}) = 1$, a zatem czynnik 2^{1-n} jest największy możliwy spośród tych zależnych tylko od n.

Nieoczywiste jest natomiast, że takie ograniczenie dolne w ogóle istnieje. Sytuacja ta bardzo się różni od podobnej, w której rozwiązań szukamy w symetrycznej kostce $|x_i| \leqslant b_i$. Wówczas, na mocy zasady szufladkowej Dirichleta, przynajmniej $\frac{1}{n}\prod_{i=1}^{k}(1 + b_i)$ z k-tek $x_1, \ldots, x_k$ spełnia

$$a_1x_1 + \cdots + a_kx_k \equiv c \pmod{n}$$

dla tej samej klasy reszt c. Niech $x_1', \ldots x_k'$ będzie jedną z nich. Wówczas każdy ciąg $x_1 - x_1', \ldots, x_k - x_k'$ jest rozwiązaniem kongruencji jednorodnej i mamy co najmniej tyleż rozwiązań w symetrycznej kostce.

Szkic rozumowania. W dowodzie hipotezy rozwijamy ideę Kaczorowskiego [Kac09], w której z kolei starał się on zaadaptować zasadę szufladkową do interesującego nas przypadku.

Przy powyższych oznaczeniach niech

$$C_n(\boldsymbol{a},\boldsymbol{b}) = \Big\{ \sum_{i=1}^{k} a_i x_i \ : \ 0 \leqslant x_i \leqslant b_i \Big\}$$

oznacza zbiór wszystkich reszt, jakie mają przynajmniej jedną reprezentację w interesującej nas kostce.

W dowodzie poszukujemy takiego ciągu $\boldsymbol{t} = (t_1, \dots, t_k)$ liczb naturalnych, że $C_n(\boldsymbol{a},\boldsymbol{t}) = C_n(\boldsymbol{a},\boldsymbol{b})$, a suma $\sum t_i$ jest możliwie niewielka (można stosunkowo łatwo pokazać, że może ona być nie większa niż $n-1$, ale nam zależy, by była ona jeszcze mniejsza). Raz jeszcze korzystajac z zasady szufladkowej wiemy, że przynajmniej $\frac{1}{n}\prod_{i=1}^{k}(1+b_i-t_i)$ k-tek $x_1, \dots, x_k$ liczb całkowitych spełnia $t_i \leqslant x_i \leqslant b_i$ oraz

$$a_1 x_1 + \dots + a_k x_k \equiv c \pmod{n}$$

dla tej samej klasy reszt c. Jeśli suma $\sum t_i$ jest istotnie mniejsza od n, to rozumując jak wyżej, dla dostatecznie dużych n mamy

$$N_n(\boldsymbol{a},\boldsymbol{b}) \geqslant \frac{1}{n}\prod_{i=1}^{k}(1+b_i-t_i) \geq 2^{1-n}\prod(1+b_i)\,.$$

Przypadki małych n zostały już rozpatrzone we wcześniejszej pracy Schinzla [Sch09, Theorem 1 and Corollary].

Znalezienie odpowiedniego ciągu $\boldsymbol{t} = (t_1, \dots, t_k)$ nie jest rzeczą bardzo trudną, choć może nieco żmudną. W tym celu, zaczynając od $\boldsymbol{t} = (0, \dots, , 0)$ staramy się w każdym kolejnym kroku zwiększyć jeden z wyrazów $\boldsymbol{t}$ o 1 tak, by zbiór $C_n(\boldsymbol{a},\boldsymbol{t})$ zwiąkszył się przynajmniej o 2 elementy. Jeśli będziemy w stanie kontynuować tę procedurę aż do znalezienia $\boldsymbol{t}$ takiego, że $|C_n(\boldsymbol{a},\boldsymbol{t})| \geqslant |C_n(\boldsymbol{a},\boldsymbol{b})| - 1$, to uzyskamy $\sum t_i \leqslant n/2$. W przeciwnym zaś razie okazuje się, i jest to clue naszego dowodu, że zbiór $C_n(\boldsymbol{a},\boldsymbol{t})$ ma dość szczególną postać, co pozwala na dokończenie rozumowania.

Ta część rozprawy oparta jest na materiale opublikowanym w pracy [CS12].

Literatura

[Bou99] J. Bourgain, *On the Dimension of Kakeya Sets and Related Maximal Inequalities*, Geometric And Functional Analysis **9** (1999), no. 2, 256–282.

[BS94] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14** (1994), no. 3, 263–268.

[Cha02] M.-C. Chang, *A polynomial bound in Freiman's theorem*, Duke Math. J. **1** (2002), 1–25.

[CS12] K. Cwalina and T. Schoen, *The number of solutions of a homogeneous linear congruence*, Acta Arith. **153** (2012), no. 3, 271–279.

[CS13a] ———, *A linear bound on the dimension in Green-Ruzsa's theorem*, J. Number Theory **133** (2013), no. 4, 1262–1269.

[CS13b] ———, *Tight bounds on additive Ramsey-type numbers*, submitted to J. Reine Angew. Math. (2013).

[Fre73] G. A. Freiman, *Foundations of a structural theory of set addition*, American Mathematical Society, Providence, RI, 1973.

[Gow98] T. W. Gowers, *A new proof of Szemeredi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), no. 3, 529–551.

[Gow01] ———, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588.

[GR07] B. J. Green and I. Z. Ruzsa, *Freiman's theorem in an arbitrary abelian group*, J. Lond. Math. Soc. **75** (2007), no. 1, 163–175.

[Kac09] J. Kaczorowski, *Appendix to Schinzel's 'The number of solutions of a linear homogeneous congruence II'*, Analytic Number Theory: essays in honour of Klaus Roth, 2009, pp. 411–413.

[Rad33] R. Rado, *Studien zur Kombinatorik*, Math. Z. **36** (1933), no. 1, 424–470.

[Ruz94] I. Z. Ruzsa, *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar. **65** (1994), no. 4, 379–388.

[San12] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

[Sch17] I. Schur, *Über die Kongruenz* $x^m + y^m \equiv z^m \pmod{p}$, Jahresber. Deutsch. Math.-Verein. **25** (1917), 114–116.

[Sch08] A. Schinzel, *The number of solutions of a linear homogeneous congruence*, Diophantine Approximation: festschrift for Wolfgang Schmidt (H. P. Schlickewei, K. Schmidt, and R. F. Tichy, eds.), Developments in Mathematics, vol. 16, Springer Vienna, Vienna, 2008.

[Sch09] ———, *The number of solutions of a linear homogeneous congruence II*, Analytic Number Theory: essays in honour of Klaus Roth, Cambridge University Press, 2009, pp. 402–413.