Ποσοτικές εκδοχές του θεωρήματος του Roth για τις αριθμητικές προόδους

Διπλωματική Εργασία

Χρήστος Φαλάρας

Τμήμα Μαθηματικών
Πανεπιστήμιο Αθηνών

Αθήνα – 2021

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

1.1 Ιστορία του προβλήματος

Ένα κεντρικό πρόβλημα στην προσθετική θεωρία αριθμών είναι να βρεθούν συνθήκες που αν ικανοποιούνται από κάποιο υποσύνολο των ακεραίων τότε αυτό περιέχει αριθμητική πρόοδο. Η πιο φυσιολογική συνθήκη που μπορεί να φανταστεί κανείς είναι ότι αν ένα σύνολο είναι αρκετά μεγάλο τότε θα περιέχει αριθμητική πρόοδο. Για να μιλήσουμε πιο συγκεκριμένα για το μέγεθος ενός συνόλου εισάγουμε την έννοια της άνω πυκνότητας.

Ορισμός 1.1.1 (άνω πυκνότητα)**.** Η άνω πυκνότητα ενός συνόλου $A \subset \mathbb{Z}$ ορίζεται να είναι το

$$\limsup_{N\to\infty} \frac{|A \cap [1, N]|}{N}.$$

Η κάτω πυκνότητα του A ορίζεται με παρόμοιο τρόπο αν αντικαταστήσουμε το $\limsup$ με $\liminf$. Αν η άνω και η κάτω πυκνότητα ενός συνόλου είναι ίσες, τότε λέμε ότι το σύνολο έχει ασυμπτωτική πυκνότητα.

Ένα από τα πρώτα αποτελέσματα της μορφής που μας ενδιαφέρει αποδείχθηκε από τον van der Waerden το 1927, ο οποίος απέδειξε ότι για κάθε ζεύγος φυσικών r και k υπάρχει $N = N(r, k)$ τέτοιος ώστε για κάθε διαμέριση του $\{1, \ldots, N\}$ σε r διακεκριμένες κλάσεις χρωμάτων, υπάρχει μονοχρωματική αριθμητική πρόοδος μήκους k. Το 1936, οι Erdős και Turán έκαναν την ισχυρότερη εικασία ότι κάθε σύνολο φυσικών που έχει θετική άνω πυκνότητα περιέχει αριθμητικές προόδους οσοδήποτε μεγάλου μήκους. Η εικασία αυτή αποδείχθηκε από τον Roth για αριθμητικές προόδους μήκους 3. Το 1969, ο Szemerédi επεξέτεινε αυτό το αποτέλεσμα σε αριθμητικές προόδους μήκους 4. Ο Roth χρησιμοποιούσε αναλυτικές μεθόδους, ενώ ο Szemerédi χρησιμοποιούσε ένα πολύπλοκο συνδυαστικό επιχείρημα. Το 1972, ο Roth τροποποίησε την αναλυτική του μέθοδο ώστε να δίνει το συμπέρασμα και για αριθμητικές προόδους μήκους 4, ενώ το 1975 ο Szemerédi τροποποίησε την συνδυαστική του μέθοδο ώστε να δίνει την πλήρη εικασία για αριθμητικές προόδους οσοδήποτε μεγάλου μήκους. Υπάρχουν πολλές διαφορετικές αποδείξεις αυτού του αποτελέσματος, το οποίο είναι πλέον γνωστό ως το θεώρημα του Szemerédi. Ανάμεσά τους, πολύ γνωστή είναι μία απόδειξη με μεθόδους εργοδικής θεωρίας, η οποία οφείλεται στους Furstenberg, Katznelson και Ornstein. Λίγο πριν το 2000, ο Gowers ανεπτυξε νέα αναλυτικά εργαλεία τα οποία οδήγησαν σε μια νέα απόδειξη του θεωρήματος του Szemerédi. Η μέθοδός του γενικεύτηκε ώστε να δουλεύει στην περίπτωση υποσυνόλων άλλων συνόλων των φυσικών. Για παράδειγμα, ο Green απέδειξε ότι κάθε σύνολο φυσικών που έχει θετική άνω σχετική πυκνότητα ως προς το σύνολο των πρώτων αριθμών περιέχει αριθμητικές προόδους μήκους 3, και αργότερα οι Green και Tao επεξέτειναν αυτό το αποτέλεσμα σε αριθμητικές προόδους οσοδήποτε μεγάλου μήκους.

1.2 Ποσοτικές εκδοχές του θεωρήματος του Roth

Το θέμα αυτής της εργασίας είναι ποσοτικές εκδοχές του θεωρήματος του Roth για αριθμητικές προόδους μήκους 3. Συμβολίζουμε με $R(N)$ τον πληθάριθμο του μεγαλύτερου υποσυνόλου του $\{1,\dots,N\}$ που δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων. Με αυτόν τον ορισμό, ο Roth (1953) απέδειξε το εξής:

Θεώρημα 1.2.1. *Ισχύει το φράγμα*

$$R(N) \ll N/\log\log N.$$

Παρουσιάζουμε το αναλυτικό επιχείρημα του Roth στο Κεφάλαιο 2.

Αργότερα δόθηκαν καλύτερα άνω φράγματα για την ποσότητα $R(N)$:

- Heath-Brown (1987), Szemerédi (1990): $R(N) \ll N/(\log n)^c$ για κάποιον $c > 0$.
- Bourgain (1999): $R(N) \ll N\sqrt{\log\log N}/\sqrt{\log N}$.
- Bourgain (2008): $R(N) \ll N(\log\log N)^2/(\log N)^{2/3}$.
- Sanders (2012): $R(N) \ll N/(\log N)^{3/4-o(1)}$.
- Sanders (2011): $R(N) \ll N(\log\log N)^6/\log N$.

Στο Κεφάλαιο 3 παρουσιάζουμε την δουλειά του Bloom, ο οποίος απέδειξε το φράγμα

$$R(N) \ll N(\log\log N)^4/\log N. \tag{1.2.1}$$

Το καλύτερο γνωστό κάτω φράγμα οφείλεται στον Behrend (1946):

$$R(N) \gg N\exp(-c\sqrt{\log N}).$$

Ο Bloom δουλεύει σε ένα πιο γενικό πλαίσιο, το οποίο του επιτρέπει να αποδείξει πιο γενικές εκδοχές του Θεωρήματος 3.1.1 τόσο στους ακεραίους όσο και στο $\mathbb{F}_q[t]$. Γενικά, ασχολείται με το πλήθος των μη τετριμμένων λύσεων εξισώσεων της μορφής

$$c_1x_1 + c_2x_2 + c_3x_3 = 0,$$

όπου $c_1+c_2+c_3 = 0$. Με τον όρο τετριμμένη λύση εννοούμε μία για την οποία $x_1 = x_2 = x_3$. Η μέθοδος του Bloom δίνει το ακόλουθο θεώρημα στους ακεραίους.

Θεώρημα 1.2.2. *Έστω c_1, c_2, c_3 μη μηδενικοί ακέραιοι τέτοιοι ώστε $c_1 + c_2 + c_3 = 0$ και $A \subset \{1, \ldots, N\}$ το οποίο δεν περιέχει μη τετριμμένες λύσεις της*

$$c_1x_1 + c_2x_2 + c_3x_3 = 0.$$

Τότε,

$$|A| \ll_{\mathbf{c}} \frac{(\log\log N)^4}{\log N}N.$$

Για να πάρουμε την (1.2.1) από το Θεώρημα 1.2.2 αρκεί να θεωρήσουμε τους συντελεστές $(c_1, c_2, c_3) = (1, 1, -2)$.

Η καινοτομία στήν εργασία του Bloom είναι ότι αποφεύγει τα συνδυαστικά εργαλεία του Sanders, και δουλεύει σχεδόν αποκλειστικά στον χώρο συχνοτήτων, με κύριο εργαλείο ένα λήμμα για τις δομικές ιδιότητες του μεγάλου φάσματος Fourier. Η ιδέα προέρχεται από την απόδειξη των Bateman και Katz για το θεώρημα του Roth στον $\mathbb{F}_p^n$. Για το σκοπό αυτό, ο Bloom αποδεικνύει μια βελτιωμένη έκδοση ενός αποτελέσματος της Chang. Συνδυάζοντας αυτό το αποτέλεσμα με την τεχνική του Sanders, μπορεί κανείς επίσης να αποδείξει ένα βελτιωμένο αποτέλεσμα για το πρόβλημα της εύρεσης αριθμητικών προόδων μεγάλου μήκους σε ένα σύνολο αθροισμάτων.

Θεώρημα 1.2.3. *Έστω $A, B \subset \{1, \ldots, N\}$ τέτοια ώστε $c_1\alpha N \leqslant |A| \leqslant |B| \leqslant c_2\alpha N$. Τότε το $A + B$ περιέχει αριθμητική πρόοδο μήκους μεγαλύτερου ή ίσου από*

$$\exp\left(cf(\alpha)\sqrt{\log N}\right),$$

όπου $f(\alpha) = \sqrt{\alpha}/\log(1/\alpha)$ και η σταθερά $c > 0$ εξαρτάται μόνο από τις c_1 και c_2.

Ο Sanders, χρησιμοποιώντας το αποτέλεσμα της Chang, είχε αποδείξει αντίστοιχο θεώρημα με $f(\alpha) = \alpha$. Το ίδιο αποτέλεσμα είχε αποδείξει ο Green με διαφορετική μέθοδο. Στη συνέχεια αυτή η εκτίμηση είχε βελτιωθεί από τους Croot, Łaba και Sisask σε $f(\alpha) = \sqrt{\alpha}(\log(1/\alpha))^{-3/2}$.

Στο Κεφάλαιο 4 παρουσιάζουμε μια πιθανοθεωρητική τεχνική των Croot και Sisask με την οποία μπορούμε να βρούμε «σχεδόν-περιόδους» συνελίξεων υποσυνόλων μιας ομάδας.

Έτσι παίρνουμε αποτελέσματα παρόμοια με τα θεωρήματα τύπου Bogolyubov που προκύπτουν με μεθόδους ανάλυσης Fourier στις αβελιανές ομάδες, χωρίς να χρειαστούμε την ύπαρξη μετασχηματισμού Fourier με καλές ιδιότητες. Το πρώτο μας αποτέλεσμα είναι το ακόλουθο θεώρημα σχεδόν περιοδικότητας.

Πρόταση 1.2.4 (L^2-σχεδόν περιοδικότητα, τοπική μορφή)**.** *Έστω G μια ομάδα, A, B πεπερασμένα υποσύνολα της G και $\varepsilon \in (0,1)$ μια παράμετρος. Υποθέτουμε ότι για κάποιο $S \subseteq G$ ισχύει ότι $|B \cdot S| \leqslant K|B|$. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T| \geqslant \frac{|S|}{(2K)^{9/\varepsilon^2}}$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \varepsilon^2 |A|\,|B|^2.$$

Η συνθήκη ότι πρέπει να υπάρχει κάποιο σύνολο S τέτοιο ώστε $|B \cdot S| \leqslant K|B|$ δικαιολογεί τον όρο «τοπική». Δεν χρειάζεται να έχουμε το B πυκνό στην G για να μπορούμε να εφαρμόσουμε αποτελεσματικά αυτή την πρόταση. Το μόνο που χρειαζόμαστε είναι το B να αλληλεπιδρά καλά με κάποιο μεγάλο σύνολο S, μια συνθήκη που θα συζητήσουμε πιο αναλυτικά παρακάτω. Ακόμα κι αν γνωρίζουμε λίγα πράγματα για τη δομή του B μπορούμε να πάρουμε χρήσιμες πληροφορίες από την πρόταση αν το B είναι πυκνό σε κάποιο δομημένο σύνολο. Για παράδειγμα, αν $G = \mathbb{Z}$ και $B \subseteq [N] := \{1, \ldots, N\}$ με $|B| \geqslant \beta N$ τότε μπορούμε να πάρουμε $S = [N]$ και $K = 2/\beta$. Όμοια, αν η G είναι πεπερασμένη τότε μπορούμε πάντα να πάρουμε $S = G$, ανεξάρτητα από το B, και έχουμε άμεσα το ακόλουθο πόρισμα.

Πόρισμα 1.2.5 (L^2-σχεδόν περιοδικότητα, ολική μορφή)**.** *Έστω G μια πεπερασμένη ομάδα, A, B υποσύνολα της G και $\varepsilon \in (0,1)$ μια παράμετρος. Υποθέτουμε ότι το B έχει πυκνότητα β. Τότε υπάρχει υποσύνολο T της G μεγέθους*

$$|T| \geqslant (\beta/2)^{9/\varepsilon^2}|G|$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \varepsilon^2 |A|\,|B|^2.$$

Τα προηγούμενα αποτελέσματα μας λένε ότι οι συνελίξεις είναι κατά κάποιον τρόπο συνεχείς. Μπορούμε να βρούμε μεγάλο πλήθος μεταφορών t ώστε η συνάρτηση $\mathbf{1}_A * \mathbf{1}_B$ να μην αλλάζει πολύ – με την L^2 έννοια – όταν την μεταφέρουμε κατά t. Έχοντας στη διάθεσή μας L^2-σχεδόν περιόδους έχουμε καλό έλεγχο για πολλές εφαρμογές, ειδικότερα σε καταστάσεις στις οποίες εμφανίζονται συνελίξεις βαθμού μεγαλύτερου από 2. Μια ενδιαφέρουσα περίπτωση είναι όταν μελετάμε το πλήθος των αριθμητικών προόδων μήκους 3 σε ένα σύνολο ή όταν μελετάμε ένα σύνολο τριπλών γινομένων $A \cdot B \cdot C$. Όμως, για κάποιες εφαρμογές στις οποίες μας ενδιαφέρει η συνήθης απλή συνέλιξη είναι πιο χρήσιμο να έχουμε L^p-σχεδόν περιόδους για μεγαλύτερες τιμές του p. Σε αυτή την κατεύθυνση έχουμε το εξής αποτέλεσμα.

Πρόταση 1.2.6 (L^p-σχεδόν περιοδικότητα, τοπική μορφή)**.** *Έστω G μια ομάδα, A, B πεπερασμένα υποσύνολα της G και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι για κάποιο $S \subseteq G$ ισχύει ότι $|B \cdot S| \leqslant K|B|$. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T| \geqslant \frac{|S|}{(2K)^{50m/\varepsilon}}$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \max\{\varepsilon^m |AB|\,|B|^m, \|\mathbf{1}_A * \mathbf{1}_B\|_m^m\}\varepsilon^m |B|^m.$$

Όπως και προηγουμένως, παίρνουμε το ακόλουθο «ολικό» πόρισμα.

Πόρισμα 1.2.7 (L^p-σχεδόν περιοδικότητα, ολική μορφή)**.** *Έστω G μια πεπερασμένη ομάδα, A, B υποσύνολα της G και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι το B έχει πυκνότητα β. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T| \geqslant (\beta/2)^{50m/\varepsilon}|G|$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \max\{\varepsilon^m |AB|\,|B|^m, \|\mathbf{1}_A * \mathbf{1}_B\|_m^m\}\varepsilon^m |B|^m.$$

Χρησιμοποιώντας αυτά τα θεωρήματα σχεδόν περιοδικότητας δείχνουμε μη-μεταθετικά ανάλογα της θεωρίας των Bogolyubov, Freiman, Halberstam, Ruzsa σχετικά με τη δομή συνόλων αθροισμάτων σε αβελιανές ομάδες.

Θεώρημα 1.2.8. *Έστω G μια ομάδα και A πεπερασμένο υποσύνολο της G τέτοιο ώστε $|A^2| \leqslant K|A|$. Για κάθε $k \geqslant 1$ υπάρχει συμμετρικό σύνολο $S \subseteq A^{-1}A$ που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $S^k \subseteq A^1 \cdot A^{-2}$ και*

$$|S| \geqslant \exp(-9k^2 K \log(2K))|A|.$$

Επιπλέον, κάθε στοιχείο του S^k έχει τουλάχιστον $|A|^3/2K$ αναπαραστάσεις της μορφής $a_1 a_2 a_3^{-1} a_4^{-1}$ με $a_i \in A$.

Με κάποια πρόσθετη προσπάθεια μπορούμε να αποδείξουμε ένα αποτέλεσμα που ισχύει για σύνολα τριπλών γινομένων. Για να το διατυπώσουμε είναι βολικό να εισαγάγουμε την ακόλουθη ορολογία: Για μια τριάδα (A, B, C) πεπερασμένων υποσυνόλων της G και ένα στοιχείο $x \in G$ λέμε ότι το x είναι γ-δημοφιλές αν

$$\mathbf{1}_A * \mathbf{1}_B * \mathbf{1}_C(x) \geqslant \gamma(|A|\,|B|)^{1/2}|C|.$$

Θεώρημα 1.2.9. *Έστω G μια ομάδα, A_1, A_2, A_3 πεπερασμένα μη κενά υποσύνολα της G και $k \geqslant 1$. Έστω x ένα $\frac{1}{K}$-δημοφιλές στοιχείο της τριάδας (A_1, A_2, A_3) και D ένα υποσύνολο της G τέτοιο ώστε $|A_3 \cdot D| \leqslant K'|A_3|$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq DD^{-1}$ που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $xS^k \subseteq A_1A_2A_3$ και*

$$|S| \geqslant \exp(-36k^2K^2\log(2K'))|D|.$$

Στην περίπτωση του γινομένου δύο συνόλων η κατάσταση μοιάζει διαφορετική. Παρόλο που δεν μπορούμε να εξασφαλίσουμε ότι υπάρχει μεταφορά ενός μεγάλου συνόλου διαδοχικών γινομένων στο $A \cdot B$, μπορούμε πάντοτε να βρούμε μια μεταφορά οποιουδήποτε μικρού υποσυνόλου ενός μεγάλου συνόλου διαδοχικών γινομένων.

Θεώρημα 1.2.10. *Έστω G μια ομάδα, A, B πεπερασμένα μη κενά υποσύνολα της G και $k, n \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι $|A \cdot B| \leqslant K|A|$ και $|B \cdot D| \leqslant K'|B|$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq DD^{-1}$ με πληθάριθμο*

$$|S| \geqslant \exp(-150k^2K\log(2K')\log(2n))|D|$$

τέτοιο ώστε το σύνολο γινομένων $A \cdot B$ να περιέχει μία αριστερή μεταφορά οποιουδήποτε συνόλου $P \subseteq S^k$ που έχει πληθάριθμο μικρότερο ή ίσο από n.

Στη συνέχεια αποδεικνύουμε ένα θεώρημα για την ύπαρξη αριθμητικών προόδων μεγάλου μήκους σε σύνολα αθροισμάτων. Ο Bourgain, χρησιμοποιώντας ανάλυση Fourier στο $\mathbb{Z}_p$, απέδειξε ότι αν A και B είναι υποσύνολα του $[N]$ με πυκνότητα α και β αντίστοιχα, τότε το $A + B$ πρέπει να περιέχει μια αριθμητική πρόοδο μήκους τουλάχιστον

$$\exp(c((\alpha\beta\log N)^{1/3} - \log\log N))$$

όπου $c > 0$ είναι μια απόλυτη σταθερά. Στη συνέχεια αυτό το κάτω φράγμα βελτιώθηκε από τον Green, και ανεξάρτητα από τον Sanders, οι οποίοι πέτυχαν τον εκθέτη $1/2$ αντί του $1/3$. Αποδεικνύουμε το ακόλουθο:

Θεώρημα 1.2.11. *Έστω N ένας θετικός ακέραιος και $A, B \subseteq [N]$ μη κενά σύνολα με πληθάριθμο αN και βN αντίστοιχα. Τότε το $A + B$ περιέχει μια αριθμητική πρόοδο μήκους τουλάχιστον*

$$\frac{1}{2}\exp\left(c\left(\frac{\alpha\log N}{\log 4/\beta}\right)^{1/4}\right)$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Μελετάμε επίσης την ποσότητα $R(N)$, το μέγιστο πλήθος που μπορεί να έχει ένα υποσύνολο του $[N] = \{1, \ldots, N\}$ το οποίο δεν περιέχει καμία αριθμητική πρόοδο τριών όρων, δηλαδή δεν περιέχει τριάδα $(x, x+d, x+2d)$ με $d \neq 0$. Χρησιμοποιώντας την πιθανοθεωρητική απόδειξη της Πρότασης 1.2.4 μπορούμε να δώσουμε καθαρά συνδυαστική απόδειξη της ακόλουθης εκδοχής του θεωρήματος του Roth.

Θεώρημα 1.2.12. *Υπάρχει συνάρτηση ω με $\omega(N) \to \infty$ όταν $N \to \infty$ τέτοια ώστε*

$$R(N) \leqslant \frac{N}{(\log\log N)^{\omega(N)}}$$

για κάθε φυσικό αριθμό N.

Κλείνουμε αυτό το κεφάλαιο με μια τελευταία εφαρμογή της πιθανοθεωρητικής τεχνικής των Croot και Sisask. Η επόμενη πρόταση δείχνει ότι τα γινόμενα συνόλων που «μοιάζουν με ομάδες» έχουν αναγκαστικά ισχυρές ιδιότητες σχεδόν περιοδικότητας.

Πρόταση 1.2.13. *Έστω A ένα πεπερασμένο υποσύνολο μιας ομάδας και έστω $\varepsilon \in (0,1)$. Υποθέτουμε ότι το A έχει την ιδιότητα ότι κάθε $x \in A^2$ έχει τουλάχιστον $|A|/K$ αναπαραστάσεις της μορφής ab με $a, b \in A$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq A^{-1}A$ με πληθάριθμο*

$$|S| \geqslant \exp(-K^2 \log(2K)\log(8/\varepsilon))|A|$$

τέτοιο ώστε, για κάθε $t \in S$,

$$|tA^2 \triangle A^2| \leqslant \varepsilon |A^2|.$$

Ο Green αποκαλεί τα σύνολα A που ικανοποιούν την υπόθεση αυτής της πρότασης «ισχυρές K-προσεγγιστικές ομάδες». Δηλαδή, το A είναι ισχυρή K-προσεγγιστική ομάδα αν $\mathbf{1}_A * \mathbf{1}_A(x) \geqslant |A|/K$ για κάθε $x \in A^2$. Προφανώς, κάθε υποομάδα μιας ομάδας είναι ισχυρή K-προσεγγιστική ομάδα με $K = 1$, υπάρχουν όμως κι άλλα, πιο πολύπλοκα, παραδείγματα.

Στο Κεφάλαιο 5 δίνουμε μια περιγραφή του ακόλουθου πολύ πρόσφατου θεωρήματος των Bloom και Sisask.

Θεώρημα 1.2.14 (Bloom-Sisask). *Έστω $N \geqslant 2$ και $A \subseteq \{1, \dots, N\}$ σύνολο που δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων, δηλαδή λύσεις της $x + y = 2z$ με $x \neq y$. Τότε*

$$|A| \ll \frac{N}{(\log n)^{1+c}},$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Είναι η πρώτη φορά που δίνεται φράγμα $o(N/\log N)$ για το πρόβλημα. Όλες οι προηγούμενες απόπειρες δεν είχαν κατορθώσει να σπάσουν το φράγμα $1/\log N$ για την πυκνότητα του A.

Το Θεώρημα 1.2.14 βρίσκει εφαρμογή σε μια πολύ γνωστή εικασία του Erdős που ισχυρίζεται ότι αν A είναι ένα σύνολο φυσικών αριθμών τέτοιο ώστε η σειρά $\sum\limits_{n\in A} \frac{1}{n}$ να αποκλίνει τότε το A περιέχει αριθμητικές προόδους οσοδήποτε μεγάλου μήκους. Ως πόρισμα του Θεωρήματος 1.2.14 παίρνουμε την πρώτη μη τετριμμένη περίπτωση αυτής της εικασίας.

Πόρισμα 1.2.15. *Έστω $A \subseteq \mathbb{N}$ τέτοιο ώστε $\sum_{n\in A} \frac{1}{n} = \infty$. Τότε το A περιέχει άπειρες το πλήθος μη τετριμμένες αριθμητικές προόδους τριών όρων.*

Έχοντας ξεπεράσει το φράγμα $1/\log N$ για την πυκνότητα, μπορούμε επίσης να βρούμε αριθμητικές προόδους τριών όρων στους πρώτους χρησιμοποιώντας απλώς την εκτίμηση του Chebyshev ότι το πλήθος των πρώτων στο $\{1, \ldots, N\}$ είναι $\gg N/\log N$. Για παράδειγμα, παίρνουμε άμεσα μια ισχυρή μορφή ενός θεωρήματος του Green: κάθε υποσύνολο των πρώτων με θετική σχετική πυκνότητα, περιέχει άπειρες το πλήθος μη τετριμμένες αριθμητικές προόδους τριών όρων. Μάλιστα, χρησιμοποιώντας απλώς την εκτίμηση του Chebyshev, παίρνουμε το εξής:

Πόρισμα 1.2.16. *Έστω $\mathbb{P}$ το σύνολο των πρώτων και έστω $A \subset \mathbb{P} \cap \{1, \ldots, N\}$. Αν το A δεν έχει μη τετριμμένες αριθμητικές προόδους τριών όρων τότε το A έχει σχετική πυκνότητα*

$$\frac{|A|}{|\mathbb{P} \cap \{1, \ldots, N\}|} \ll \frac{1}{(\log N)^c}$$

για κάποια απόλυτη σταθερά $c > 0$.

ΚΕΦΑΛΑΙΟ 2

Το θεώρημα του Roth

2.1 Πρώτη απόδειξη του θεωρήματος

Η διατύπωση του κλασικού θεωρήματος του Roth είναι η ακόλουθη.

Θεώρημα 2.1.1 (Roth). *Υπάρχει σταθερά $c > 0$ τέτοια ώστε για κάθε x αρκετά μεγάλο, αν S είναι ένα υποσύνολο του συνόλου των ακεραίων στο $[1, x]$ με τουλάχιστον $cx/\log\log x$ στοιχεία, τότε το S περιέχει αριθμητική πρόοδο με τρεις όρους.*

Πριν την απόδειξη θα κάνουμε κάποιες αρχικές παρατηρήσεις. Αν f είναι μια συνάρτηση από το $\mathbb{Z}_N$ στο $\mathbb{C}$, ορίζεται ο μετασχηματισμός Fourier της f ως εξής:

$$\widehat{f}(a) = \sum_{n=0}^{N-1} f(n)\omega^{an},$$

όπου $\omega = e^{2\pi i/N}$. Αν η f είναι η δείκτρια συνάρτηση κάποιου συνόλου S τότε

$$\sum_{a=0}^{N-1} \widehat{f}(a) = N|S|,$$

αφού για κάθε $n \in S$ έχουμε $f(n) = 1$ και για σταθερό n είναι $\sum_{a=0}^{N-1} \omega^{an} = 0$ αν και μόνο αν $n \neq 0$.

Γράφοντας 3-ΑΠ θα εννοούμε μια τριάδα αριθμών $(u, v, w) \in S \times S \times S$ τέτοια ώστε $u + w = 2v$. Αν είναι $u = v = w$ θα τη λέμε εκφυλισμένη. Σημειώνουμε ότι οι γραμμικοί μετασχηματισμοί διατηρούν τις αριθμητικές προόδους, με την εξής έννοια:

$$au + b + aw + b = a(u + w) + 2b = 2av + 2b = 2(av + b).$$

Τέλος, αν $A \subseteq B$ ορίζουμε ως πυκνότητα του A στο B την ποσότητα $|A|/|B|$.

Απόδειξη. Υποθέτουμε ότι $|S| = \varepsilon x$, δηλαδή η πυκνότητα του S στο $[1,x]$ είναι ε, και $N = 2x$. Τότε το σύνολο των 3-ΑΠ του S συμπίπτει με το σύνολο των 3-ΑΠ του $S \bmod N$. Τώρα, θεωρούμε τη δείκτρια συνάρτηση του S που ορίζεται ως εξής:

$$S(n) = \begin{cases} 1 & , \quad \text{αν } n \in S \\ 0 & , \quad \text{αν } n \notin S \end{cases}.$$

Βλέπουμε την $S(n)$ ως συνάρτηση στο $\mathbb{Z}_N$ και παίρνουμε το μετασχηματισμό Fourier $\widehat{S}(a)$. Ακόμα θεωρούμε τη συνάρτηση

$$f(n) = \begin{cases} \varepsilon & , \quad \text{αν } 1 \leq n \leq x \\ 0 & , \quad \text{αν } x \leq n \leq N-1 \text{ ή } n = 0 \end{cases}$$

και την $T(x) = S(n) - f(n)$. Οι βασικές ιδιότητες της f είναι ότι $f = S = 0$, αν $x \leq n \leq N-1$ και

$$\sum_n f(n) = \sum_n S(n) = \varepsilon x.$$

Τώρα έχουμε

$$\begin{aligned} \frac{1}{N}\sum_{a=0}^{N-1} \widehat{S}(a)^2 \widehat{T}(-2a) &= \frac{1}{N}\sum_{a=0}^{N-1} \widehat{S}(a)^2 \widehat{S}(-2a) - \frac{1}{N}\sum_{a=0}^{N-1} \widehat{S}(a)^2 \widehat{f}(-2a) \\ &= (\text{πλήθος 3-ΑΠ στο } S) - \varepsilon(O^2 + E^2) \\ &\leq (\text{πλήθος 3-ΑΠ στο } S) - \varepsilon\frac{|S|^2}{2}, \end{aligned}$$

όπου O είναι το πλήθος των περιττών ακεραίων στο S και E είναι το πλήθος των άρτιων ακεραίων στο S. Η ποσότητα $O^2 + E^2$ ισούται με το πλήθος των διατεταγμένων ζευγών $(u,v) \in S \times S$ με την ιδιότητα ότι οι u και v είναι και οι δύο περιττοί ή και οι δύο άρτιοι. Με τον όρο 3-ΑΠ εννοούμε μια τριάδα $(u,v,w) \in S \times S \times S$ που ικανοποιεί την $u + v = 2w$, δηλαδή στο πλήθος των 3-ΑΠ συμπεριλαμβάνουμε και τις εκφυλισμένες.

Τώρα το κεντρικό επιχείρημα για την απόδειξη είναι το εξής: Είτε όλοι οι συντελεστές Fourier της T θα είναι «μικροί» και θα μπορούμε να βρούμε μια 3-ΑΠ μέσα στο S, είτε μπορούμε να βρούμε μια αριθμητική πρόοδο P μέσα στο $[1,x]$ με $|P| > \sqrt{x}/\log x$ τέτοια ώστε το S να έχει αυξημένη πυκνότητα στην P, δηλαδή

$$\frac{|S \cap P|}{|P|} > \varepsilon \ (1 + \delta/2)$$

για κάποιο $\delta > 0$ που θα επιλέξουμε κατάλληλα. Θα δούμε ότι αν εφαρμόσουμε διαδοχικά αυτό το επιχείρημα οδηγούμαστε σε άτοπο, άρα το S πρέπει να περιέχει μη εκφυλισμμένες 3-ΑΠ.

Υποθέτουμε ότι για κάθε $a = 0, \dots, N-1$ ισχύει

$$|\widehat{T}(a)| < \delta S \tag{2.1.1}$$

Τότε

$$\frac{1}{N}\Big|\sum_{a=0}^{N-1}\widehat{S}(a)^2\widehat{T}(-2a)\Big| < \frac{\delta S}{N}\sum_{a=0}^{N-1}|\widehat{S}(a)|^2 = \delta|S|^2 \tag{2.1.2}$$

από την ταυτότητα Parseval. Συνδυάζοντας με την (2.1.1) λαμβάνουμε:

$$(\text{πλήθος των 3-ΑΠ στο } S) \geq \frac{\varepsilon|S|^2}{2} - \delta|S|^2.$$

Για $\delta < \varepsilon/3$, παρατηρώντας ότι οι τετριμμένες 3-ΑΠ έχουν πλήθος $|S|$, συμπεραίνουμε ότι το S περιέχει μη τετριμμένες 3-ΑΠ, όπως θέλαμε να δείξουμε.

Υποθέτοντας ότι η (2.1.1) δεν ισχύει, θα δείξουμε ότι υπάρχει πρόοδος P με τις προαναφερθείσες ιδιότητες. Έστω λοιπόν ότι για κάποιο a δεν ισχύει η (2.1.1). Ισχυριζόμαστε ότι υπάρχει ακέραιος d, $1 \leq d \leq \sqrt{x}$ ώστε $da/N \equiv \gamma \pmod 1$ με την έννοια ότι η ποσότητα da/N είναι $1/\sqrt{x}$ κοντά σε κάποιον ακέραιο. Αφού το σύνολο περιέχει περισσότερα από $1/\sqrt{x}$ στοιχεία, υπάρχουν $O \leq j_1 \leq j_2 \leq \sqrt{x}$ με $j_1a/N \equiv j_2a/N + \gamma \pmod 1$. Θέτοντας $d = j_1 - j_2$ έχουμε το ζητούμενο.

Τώρα έχουμε ότι για κάθε $0 \leq j \leq \sqrt{x}/\log x$

$$\omega^{(b+jd)a} = \omega^b\omega^{jba} = \omega^b(1 + O(j/\sqrt{x})) = \omega^b + O(1/\log x),$$

αφού το δεκαδικό μέρος του jda/N είναι το πολύ $j/\sqrt{x}$. Τώρα θεωρούμε το άθροισμα

$$\begin{aligned}
F &= \sum_{1\leq b\leq x(1-1/\log x)}\Big|\sum_{0\leq j\leq\sqrt{x}/\log x}(S(b+jd) - f(b+jd))\omega^{(b+jd)a}\Big| + O(x\sqrt{x}/\log^2 x)\\
&\geq \Big|\sum_{1\leq b\leq x(1-1/\log x)}\sum_{0\leq j\leq\sqrt{x}/\log x} T(b+jd)\omega^{(b+jd)a}\Big| + O(x\sqrt{x}/\log^2 x)\\
&= \Big|\sum_{n\leq x} r(n)T(n)\omega^{an}\Big| + O(x\sqrt{x}/\log^2 x),
\end{aligned}$$

όπου $r(n)$ είναι τα ζευγάρια ακεραίων (b, j) με $0 \leq j \leq \sqrt{x}/\log x$ και $1 \leq b \leq x(1-1/\log x)$ που ικανοποιούν την $b + jd = n$. Τώρα για $n \in [x/\log x, (1-1/\log x)]x$ έχουμε ότι $r(n) = \lfloor\sqrt{x}/\log x\rfloor + 1$. Άρα,

$$F > (\sqrt{x}/\log x)\ \Big|\sum_{n\leq x} T(n)\omega^{an}\Big| + O(x\sqrt{x}/\log^2 x) > \frac{\delta\varepsilon x\sqrt{x}}{\log x} + O(x\sqrt{x}/\log^2 x).$$

Άρα, για κάποιον ακέραιο $1 \le b \le x(1 - 1/\log x)$ ισχύει

$$\sum_{0\le j\le \sqrt{x}/\log x} (S(b+jd) - f(b+jd)) > \frac{\delta\varepsilon\sqrt{x}}{\log x} + O(\sqrt{x}/\log^2 x).$$

Γι' αυτά τα j έχουμε $f(b+jd) = \varepsilon$, άρα

$$\sum_{0\le j\le \sqrt{x}/\log x} S(b+jd) > \frac{\varepsilon\sqrt{x}}{\log x}\ (1+\delta/2)$$

για κατάλληλα μεγάλο x. Άρα το S έχει πυκνότητα τουλάχιστον $\varepsilon(1+\delta/2)$ στην πρόοδο $P = \{b + jd : 0 \le j \le \sqrt{x}/\log x\}$, όπως θέλαμε να δείξουμε.

Τώρα η απόδειξη ολοκληρώνεται ως εξής. Μεταφέρουμε και αλλάζουμε κλίμακα στην πρόοδο P. Αν A είναι μια 3-ΑΠ στο S_2 τότε το S έχει 3-ΑΠ, αφού αυτές διατηρούνται από γραμμικούς μετασχηματισμούς. Επαναλαμβάνουμε το επιχείρημα, οπότε είτε θα προκύψει κάποιο σύνολο που θα έχει 3-ΑΠ, είτε θα έχουμε μια ακολουθία συνόλων S_n, $n = 1, 2, \ldots, k$ με $k > a(\log\log x)$, $a > 0$, ώστε για κάθε $i = 2, \ldots, k$ να ισχύει

$$\frac{S_i}{y_i} > (1+\delta/2)\frac{S_{i-1}}{y_{i-1}}, \text{ όπου } y_i = \sqrt{y_{i-1}}/\log y_i - 1.$$

Αυτό δεν μπορεί να ισχύει για σταθερό $\varepsilon \in (0,1]$. Για κατάλληλα μεγάλο x και για $\delta = \varepsilon/3$ έχουμε

$$\frac{S_k}{y_k} > (1+\delta/2)^{k-1}\varepsilon > \varepsilon\exp(c_1\varepsilon\log\log x) > 1.$$

Άρα αν $|S| > cx/\log\log x$ το S περιέχει 3-ΑΠ. $\square$

ΚΕΦΑΛΑΙΟ 3

Γενικεύσεις και βελτιωμένες εκτιμήσεις

3.1 Εισαγωγή

Σε αυτό το κεφάλαιο παρουσιάζουμε τη δουλειά του Bloom, ο οποίος απέδειξε την ακόλουθη βελτιωμένη έκδοση του θεωρήματος του Roth.

Θεώρημα 3.1.1. *Έστω $A \subset \{1, \ldots, N\}$ το οποίο δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων. Τότε,*

$$|A| \ll \frac{(\log\log N)^4}{\log N} N.$$

Συμβολίζουμε με $R(N)$ τον πληθάριθμο του μεγαλύτερου υποσυνόλου του $\{1, \ldots, N\}$ που δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων. Με αυτόν τον ορισμό, τα προηγούμενα άνω φράγματα για τον $R(N)$ είναι τα ακόλουθα:

- Roth (1953): $R(N) \ll N/\log\log N$.
- Heath-Brown (1987), Szemerédi (1990): $R(N) \ll N/(\log n)^c$ για κάποιον $c > 0$.
- Bourgain (1999): $R(N) \ll N\sqrt{\log\log N}/\sqrt{\log N}$.
- Bourgain (2008): $R(N) \ll N(\log\log N)^2/(\log N)^{2/3}$.
- Sanders (2012): $R(N) \ll N/(\log N)^{3/4-o(1)}$.
- Sanders (2011): $R(N) \ll N(\log\log N)^6/\log N$.

Το Θεώρημα 3.1.1 δίνει την εκτίμηση

$$R(N) \ll N(\log\log N)^4/\log N.$$

Το καλύτερο γνωστό κάτω φράγμα οφείλεται στον Behrend (1946):

$$R(N) \gg N\exp(-c\sqrt{\log N}).$$

Η καινοτομία στήν εργασία του Bloom είναι ότι αποφεύγει τα συνδυαστικά εργαλεία του Sanders, και δουλεύει σχεδόν αποκλειστικά στον χώρο συχνοτήτων, με κύριο εργαλείο ένα λήμμα για τις δομικές ιδιότητες του μεγάλου φάσματος Fourier. Η ιδέα προέρχεται από την απόδειξη των Bateman και Katz για το θεώρημα του Roth στον $\mathbb{F}_p^n$. Για το σκοπό αυτό, ο Bloom αποδεικνύει μια βελτιωμένη έκδοση ενός αποτελέσματος της Chang. Συνδυάζοντας αυτό το αποτέλεσμα με την τεχνική του Sanders, μπορεί κανείς επίσης να αποδείξει ένα βελτιωμένο αποτέλεσμα για το πρόβλημα της εύρεσης αριθμητικών προόδων μεγάλου μήκους σε ένα σύνολο αθροισμάτων.

Θεώρημα 3.1.2. *Έστω $A,B \subset \{1,\dots,N\}$ τέτοια ώστε $c_1\alpha N \leqslant |A| \leqslant |B| \leqslant c_2\alpha N$. Τότε το $A+B$ περιέχει αριθμητική πρόοδο μήκους μεγαλύτερου ή ίσου από*

$$\exp\Big(cf(\alpha)\sqrt{\log N}\Big),$$

όπου $f(\alpha)=\sqrt{\alpha}/\log(1/\alpha)$ και η σταθερά $c>0$ εξαρτάται μόνο από τις c_1 και c_2.

Ο Sanders, χρησιμοποιώντας το αποτέλεσμα της Chang, είχε αποδείξει αντίστοιχο θεώρημα με $f(\alpha)=\alpha$. Το ίδιο αποτέλεσμα είχε αποδείξει ο Green με διαφορετική μέθοδο. Στη συνέχεια αυτή η εκτίμηση είχε βελτιωθεί από τους Croot, Łaba και Sisask σε $f(\alpha)=\sqrt{\alpha}(\log(1/\alpha))^{-3/2}$.

Ο Bloom δουλεύει σε ένα πιο γενικό πλαίσιο, το οποίο του επιτρέπει να αποδείξει πιο γενικές εκδοχές του Θεωρήματος 3.1.1 τόσο στους ακεραίους όσο και στο $\mathbb{F}_q[t]$. Γενικά, ασχολείται με το πλήθος των μη τετριμμένων λύσεων εξισώσεων της μορφής

$$c_1x_1+c_2x_2+c_3x_3=0, \tag{3.1.1}$$

όπου $c_1+c_2+c_3=0$. Με τον όρο τετριμμένη λύση εννοούμε μία για την οποία $x_1=x_2=x_3$. Η μέθοδος του Bloom δίνει το ακόλουθο θεώρημα στους ακεραίους.

Θεώρημα 3.1.3. *Έστω c_1,c_2,c_3 μη μηδενικοί ακέραιοι τέτοιοι ώστε $c_1+c_2+c_3=0$ και $A\subset\{1,\dots,N\}$ το οποίο δεν περιέχει μη τετριμμένες λύσεις της*

$$c_1x_1+c_2x_2+c_3x_3=0.$$

Τότε,

$$|A| \ll_{\mathbf{c}} \frac{(\log\log N)^4}{\log N}N.$$

Το Θεώρημα 3.1.1 προκύπτει από το Θεώρημα 3.1.3 αν θεωρήσουμε τους συντελεστές $(c_1, c_2, c_3) = (1, 1, -2)$.

Στην περίπτωση του πολυωνυμικού δακτυλίου $\mathbb{F}_q[t]$ η ίδια μέθοδος δίνει ένα ελαφρώς ισχυρότερο αποτέλεσμα.

Θεώρημα 3.1.4. *Έστω $A \subset \mathbb{F}_q[t]_{\deg<n}$. Αν τα $c_1, c_2, c_3 \in \mathbb{F}_q[t] \setminus \{0\}$ ικανοποιούν την $c_1 + c_2 + c_3 = 0$ και το $A \subset \{1, \ldots, N\}$ δεν περιέχει μη τετριμμένες λύσεις της $c_1x_1 + c_2x_2 + c_3x_3 = 0$, τότε*

$$|A| \ll_{\mathbf{c}} \frac{(\log n)^2}{n} q^n.$$

Στην περίπτωση όπου $c_1, c_2, c_3 \in \mathbb{F}_q \setminus \{0\}$, το πρόβλημα είναι πολύ απλούστερο και υπάρχουν ισχυρότερα αποτελέσματα. Οι Liu και Spencer απέδειξαν το 2009 ότι ισχύει το άνω φράγμα $|A| \ll_{\mathbf{c}} q^n/n$.

Το βασικό τεχνικό αποτέλεσμα στη δουλειά του Bloom είναι μια ποιοτικά ισχυρότερη εναλλακτική εκδοχή ενός γνωστού λήμματος της Chang που αφορά την προσθετική δομή του μεγάλου φάσματος του μετασχηματισμού Fourier σε πεπερασμένες ομάδες. Αν G είναι μια πεπερασμένη αβελιανή ομάδα και A είναι ένα υποσύνολο της G με πυκνότητα $\alpha = |A|/|G|$, ορίζουμε το μεγάλο φάσμα $\Delta_\eta(G)$ ως το σύνολο των χαρακτήρων $\gamma \in \widehat{G}$ για τους οποίους $|\widehat{A}(\gamma)| \geqslant \eta|A|$. Από την ταυτότητα Parseval έπεται άμεσα ότι

$$|\Delta_\eta(A)| \leqslant \eta^{-2}\alpha^{-1},$$

και αυτό είναι το καλύτερο άνω φράγμα που μπορούμε να δώσουμε για τον πληθάριθμο. Το λήμμα της Chang δείχνει ότι μπορούμε να βρούμε ένα μικρότερο σύνολο το οποίο «ελέγχει» προσθετικά το φάσμα. Πιο συγκεκριμένα, λέμε ότι το Δ έχει d-κάλυψη αν υπάρχει Λ με πληθάριθμο $|\Lambda| \leqslant d$ τέτοιο ώστε

$$\Delta \subset \left\{ \sum_{\lambda\in\Lambda} \varepsilon_\lambda \lambda : \varepsilon_\lambda \in \{-1, 0, 1\} \right\}.$$

Με αυτή την ορολογία το λήμμα της Chang διατυπώνεται ως εξής:

Θεώρημα 3.1.5 (Chang)**.** *Αν το $A \subset G$ έχει πυκνότητα $\alpha = |A|/|G|$ τότε το $\Delta_\eta(A)$ έχει d-κάλυψη για κάποιον*

$$d \ll \eta^{-2} \log(1/\alpha).$$

Η μέθοδος του Bloom, σε αντίθεση με προηγούμενες βελτιώσεις του θεωρήματος του Roth, δεν κάνει απευθείας χρήση του λήμματος της Chang. Χρησιμοποιεί το ακόλουθο θεώρημα το οποίο, για κάποιες εφαρμογές, είναι πολύ ισχυρότερο.

Θεώρημα 3.1.6. *Αν το $A \subset G$ έχει πυκνότητα $\alpha = |A|/|G|$ τότε υπάρχει $\Delta' \subset \Delta_\eta(A)$ με πληθάριθμο $|\Delta'| \gg \eta|\Delta_\eta(A)|$ το οποίο έχει d-κάλυψη για κάποιον*

$$d \ll \eta^{-1}\log(1/\alpha).$$

Με άλλα λόγια, μπορούμε να κερδίσουμε έναν παράγοντα η στη διάσταση χάνοντας μόνο έναν παράγοντα η στον πληθάριθμο του συνόλου που θεωρούμε. Θα αποδείξουμε το Θεώρημα 3.1.6 (για την ακρίβεια, μια γενικότερη έκδοσή του) θεωρώντας την προσθετική ενέργεια των μεγάλων φασμάτων, επεκτείνοντας ιδέες των Shkredov και Bateman-Katz. Θα συζητήσουμε τις ιδέες που οδηγούν στο Θεώρημα 3.1.6 σε ένα γενικό πλαίσιο το οποίο επίσης δουλεύει για καλύψεις «ως προς» δοθέν σύνολο, κάτι που χρειάζεται για την στρατηγική αύξησης της πυκνότητας που χρησιμοποιείται στην απόδειξη του θεωρήματος του Roth.

3.2 Ορισμοί

Έστω G μια πεπερασμένη αβελιανή ομάδα και $\widehat{G}$ η δυϊκή της ομάδα. Θέτουμε $N = |G|$. Θα χρησιμοποιούμε το μέτρο απαρίθμησης στην G και την $\widehat{G}$. Ειδικότερα, οι L^p-νόρμες στην G και την $\widehat{G}$ ορίζονται ως εξής: αν $f : G \to \mathbb{C}$ είναι μια συνάρτηση και $p \geqslant 1$ τότε

$$\|f\|_p = \left(\sum_{x\in G}|f(x)|^p\right)^{1/p} \quad \text{και} \quad \|f\|_\infty = \sup_{x\in G}|f(x)|.$$

Όμοια ορίζεται η L^p-νόρμα μιας συνάρτησης $\omega : \widehat{G} \to \mathbb{C}$. Για κάθε συνάρτηση $f : G \to \mathbb{C}$ ορίζουμε τον μετασχηματισμό Fourier $\widehat{f} : \widehat{G} \to \mathbb{C}$ με

$$\widehat{f}(\gamma) = \sum_x f(x)\gamma(x).$$

Για κάθε ζεύγος συναρτήσεων $f, g : G \to \mathbb{C}$ ισχύει η ταυτότητα Parseval

$$\langle f, g\rangle = \sum_x f(x)\overline{g(x)} = \frac{1}{N}\sum_\gamma \widehat{f}(\gamma)\overline{\widehat{g}(\gamma)}.$$

Έστω $B \subset G$ και $\Gamma \subset \widehat{G}$. Για δοθέν $\varepsilon \in [0, 2]$ λέμε ότι το B έχει τον ε-έλεγχο του Γ αν για κάθε $x \in B$ και $\gamma \in \Gamma$ ισχύει

$$|1 - \gamma(x)| \leqslant \varepsilon.$$

Για κάθε $\eta \in [0, 1]$ και $f : G \to \mathbb{C}$ ορίζουμε το φάσμα

$$\Delta_\eta(f) = \{\gamma \in \widehat{G} : |\widehat{f}(\gamma)| \geqslant \eta\|f\|_1\}.$$

Θέτουμε επίσης
$$\tilde{\Delta}_\eta(f) = \{\gamma \in \widehat{G} : \eta\|f\|_1 \leqslant |\widehat{f}(\gamma)| < 2\eta\|f\|_1\}.$$

Αν $0 < \delta \leqslant 1$ συμβολίζουμε με $\mathcal{L}(\delta)$ την ποσότητα $2 + \lceil \log(1/\delta) \rceil$. Επίσης, για κάθε $A \subset G$ ορίζουμε $\beta(A) = |A \cap B|/|B|$. Θα λέμε ότι το $A \subset B$ έχει σχετική πυκνότητα α αν $\beta(A) = \alpha$. Συχνά θα ταυτίζουμε ένα σύνολο με τη δείκτρια συνάρτησή του. Για παράδειγμα, αν $\Gamma \subset \widehat{G}$ θα γράφουμε $\Gamma(\gamma) = 1$ αν $\gamma \in \Gamma$ και 0 αλλιώς.

Έστω $\Gamma \subset \widehat{G}$ και $\omega : \widehat{G} \to \mathbb{R}^+$. Για κάθε ακέραιο $m \geqslant 1$ ορίζουμε την προσθετική ενέργεια
$$E_{2m}(\omega, \Gamma) = \sum_{\gamma_1, \ldots, \gamma'_m} \omega(\gamma_1) \cdots \omega(\gamma'_m) \Gamma\left(\sum_{i=1}^m \gamma_i - \sum_{j=1}^m \gamma'_j\right)$$
και την περιορισμένη ενέργεια
$$E^{\#}_{t_1,t_2}(\omega, \Gamma) = \sum_{|\Delta_1|=t_1, |\Delta_2|=t_2, \Delta_1 \cap \Delta_2 = \varnothing} \prod_{\gamma \in \Delta_1 \cup \Delta_2} \omega(\gamma) \Gamma\left(\sum_{\gamma \in \Delta_1} \gamma - \sum_{\gamma' \in \Delta_2} \gamma'\right).$$

Θέτουμε $E^{\#}_{2m} := E^{\#}_{m,m}$ και για κάθε ω και Γ ορίζουμε $E_0(\omega, \Gamma) = E^{\#}_0(\omega, \Gamma) = 1$. Παρατηρήστε ότι οι E και $E^{\#}$ διαφέρουν, όχι μόνο στον περιορισμό για την επανάληψη στοιχείων, αλλά και στο ότι η πρώτη επηρεάζεται από τις μεταθέσεις των γ_i.

Λέμε ότι το S έχει d-κάλυψη από το Γ αν υπάρχει $\Lambda \subset \widehat{G}$ με πληθάριθμο $|\Lambda| \leqslant d$ τέτοιο ώστε
$$S \subset \Gamma - \Gamma + \langle \Lambda \rangle,$$
όπου
$$\langle \Lambda \rangle = \left\{ \sum_{\lambda \in \Lambda} \varepsilon_\lambda \lambda : \varepsilon_\lambda \in \{-1, 0, 1\} \right\}$$
και $\langle \varnothing \rangle = \{0\}$.

Λέμε ότι το Δ είναι Γ-αποσυνδεδεμένο αν για κάθε $k \geqslant 1$ και $\lambda \in \widehat{G}$ υπάρχουν το πολύ 2^k ζεύγη Δ_1, Δ_2 ξένων υποσυνόλων του Δ με $|\Delta_1 \cup \Delta_2| = k$ και
$$\sum_{\gamma \in \Delta_1} \gamma - \sum_{\gamma' \in \Delta_2} \gamma' \in \Gamma + \lambda.$$

Τέλος, λέμε ότι το S έχει Γ-διάσταση ίση με d αν d είναι το μέγεθος του μεγαλύτερου Γ-αποσυνδεδεμένου υποσυνόλου του S. Παρατηρήστε ότι η διάσταση είναι πάντα τουλάχιστον 1 διότι κάθε μονοσύνολο είναι τετριμμένα Γ-αποσυνδεδεμένο για κάθε $\Gamma \subset \widehat{G}$. Παρατηρήστε επίσης ότι αν το Δ είναι Γ-αποσυνδεδεμένο τότε είναι επίσης Γ'-αποσυνδεδεμένο για κάθε μεταφορά Γ' του Γ.

3.3 Προσθετική ενέργεια

Σε αυτή την ενότητα μελετάμε τη σχέση ανάμεσα στη διάσταση ενός συνόλου και την προσθετική του ενέργεια. Αν ένα σύνολο έχει πολύ μεγάλη διάσταση τότε σχεδόν ολόκληρο το σύνολο είναι αποσυνδεδεμένο και θα περιμέναμε λίγες προσθετικές σχέσεις μεταξύ των στοιχείων του, άρα θα έπρεπε να έχει μικρή προσθετική ενέργεια. Το λήμμα που ακολουθεί επιβεβαιώνει αυτή τη διαισθητική πρόβλεψη.

Λήμμα 3.3.1. *Έστω $S \subset \widehat{G}$ με Γ-διάσταση $|S| = k$. Τότε, για κάθε $m \geqslant t_1, t_2 \geqslant 0$,*

$$E^{\#}_{t_1,t_2}(S,\Gamma) \leqslant 4^{k+m}.$$

Απόδειξη. Έστω ότι $S = S_0 \bigsqcup S_1$, όπου το S_0 είναι Γ-αποσυνδεδεμένο και $|S_1| = k$. Ξεχωρίζοντας τη συμβολή των υποσυνόλων του S_1 παίρνουμε την εκτίμηση

$$\begin{aligned} E^{\#}_{t_1,t_2}(S,\Gamma) &= \sum_{|\Delta_1|=t_1, |\Delta_2|=t_2, \Delta_1\cap\Delta_2=\varnothing} \Gamma\left(\sum_{\gamma\in\Delta_1}\gamma - \sum_{\gamma'\in\Delta_2}\gamma'\right) \\ &\leqslant \sum_{0\leqslant r_i\leqslant t_i} \binom{k}{r_1}\binom{k}{r_2} \sup_{\lambda} \sum_{\Delta_i\in\binom{S_0}{t_i-r_i}, \Delta_1\cap\Delta_2=\varnothing} \Gamma\left(\sum_{\gamma\in\Delta_1}\gamma - \sum_{\gamma'\in\Delta_2}\gamma' + \lambda\right). \end{aligned}$$

Αφού το S_0 είναι Γ-αποσυνδεδεμένο, ο εσωτερικός προσθετέος φράσσεται από $2^{t_1+t_2}$ και έχουμε το λήμμα. □

Το επόμενο λήμμα μας επιτρέπει να αξιοποιήσουμε πληροφορίες για την περιορισμένη προσθετική ενέργεια ώστε να καταλήξουμε σε συμπεράσματα για την πλήρη προσθετική ενέργεια.

Λήμμα 3.3.2. *Για κάθε $\Gamma \subset \widehat{G}$, κάθε συνάρτηση βάρους $\omega : \widehat{G} \to \mathbb{R}^+$ και κάθε ακέραιο $m \geqslant 2$ έχουμε*

$$E_{2m}(\omega,\Gamma) \leqslant 2^{4m}(m!)^2\|\omega\|_2^{2m} \sum_{0\leqslant t_1,t_2\leqslant m} \frac{\|\omega\|_2^{-t_1-t_2}}{((m-t_1)!(m-t_2)!)^{1/2}} \sup_{\lambda} E^{\#}_{t_1,t_2}(\omega,\Gamma+\lambda).$$

Απόδειξη. Χωρίζουμε σε ομάδες τους προσθετέους του E_{2m} σύμφωνα με το μέγεθος των υποσυνόλων των $\{\gamma_1,\dots,\gamma_m\}$ και $\{\gamma'_1,\dots,\gamma'_m\}$ που αποτελούνται από στοιχεία που το καθένα εμφανίζεται με πολλαπλότητα 1. Παίρνουμε έτσι το άνω φράγμα

$$E_{2m}(\omega,\Gamma) \leqslant \sum_{0\leqslant \ell_1,\ell_2\leqslant m} G_{m-\ell_1}(\omega)G_{m-\ell_2}(\omega)\binom{m}{\ell_1}\binom{m}{\ell_2} \sup_{\lambda} F_{\lambda}(\ell_1,\ell_2) \tag{3.3.1}$$

όπου

$$F_\lambda(\ell_1,\ell_2)=\sum_{\substack{\gamma_1,\dots,\gamma'_{\ell_2}\\ \gamma_i\neq\gamma_j,\gamma'_i\neq\gamma'_j,i\neq j}}\omega(\gamma_1)\cdots\omega(\gamma'_{\ell_2})\Gamma\left(\sum_{i=1}^{\ell_1}\gamma_i-\sum_{j=1}^{\ell_2}\gamma'_j-\lambda\right)$$

και

$$G_k(\omega)=\sum_{\Delta}^{*}\prod_{\gamma\in\Delta}\omega(\gamma)\leqslant\frac{k!}{(\lfloor k/2\rfloor)!}\left(\sum_{\gamma}\omega(\gamma)62\right)^{k/2},\tag{3.3.2}$$

όπου το πρώτο άθροισμα είναι περιορισμένο σε εκείνες τις διατεταγμένες k-άδες $\Delta\in\widehat{G}^k$ στις οποίες κάθε στοιχείο εμφανίζεται με πολλαπλότητα τουλάχιστον 2. Το άθροισμα $F_\lambda(\ell_1,\ell_2)$ ουσιαστικά μια ανα-κανονικοποιημένη έκδοση της περιορισμένης ενέργειας $E^{\#}_{t_1,t_2}$ με τη διαφορά ότι λείπει ο περιορισμός $\gamma_i\neq\gamma'_j$ για κάθε $1\leqslant i\leqslant\ell_1$ και $1\leqslant j\leqslant\ell_2$. Για να τον συμπεριλάβουμε, χωρίζουμε το $F_\lambda(\ell_1,\ell_2)$ σύμφωνα με το πλήθος των κοινών στοιχείων μεταξύ των γ_i και γ'_j. Έτσι, έχουμε

$$F_\lambda(\ell_1,\ell_2)\leqslant\sum_{i=0}^{\min(\ell_1,ell_2)}\binom{\ell_1}{i}\binom{\ell_2}{j}i!\|\omega\|_2^{2i}(\ell_1-i)!(\ell_2-i)!E^{\#}_{\ell_1-i,\ell_2-i}(\omega,\Gamma+\lambda).\tag{3.3.3}$$

Συνδυάζοντας τις (3.3.1), (3.3.2) και (3.3.3) και απλοποιώντας αυτή την παράσταση βλέπουμε ότι το $E_{2m}(\omega,\Gamma)$ φράσσεται από

$$(m!)^2\|\omega\|_2^{2m}\sum_{0\leqslant\ell_1,\ell_2\leqslant m}\sum_{i=0}^{\min(\ell_1,\ell_2)}\frac{\|\omega\|_2^{2i-\ell_1-\ell_2}}{i!(\lfloor(m-\ell_1)/2\rfloor)!(\lfloor(m-\ell_2)/2\rfloor)!}\sup_\lambda E^{\#}_{\ell_1-i,\ell_2-i}(\omega,\Gamma+\lambda).$$

Θέτοντας $t_1=\ell_1-i$ και $t_2=\ell_2-i$ βλέπουμε ότι αυτή η ποσότητα φράσσεται από

$$(m!)^2\|\omega\|_2^{2m}\sum_{0\leqslant t_1,t_2\leqslant m}\|\omega\|_2^{-t_1-t_2}\sup_\lambda E^{\#}_{t_1,t_2}(\omega,\Gamma+\lambda)f(m,t_1,t_2)$$

όπου

$$f(m,t_1,t_2)=\sum_{i\geqslant\max(t_1,t_2)}^{m-\max(t_1,t_2)}\frac{1}{i!(\lfloor(m-t_1-i)/2\rfloor)!(\lfloor(m-t_2-i)/2\rfloor)!}.$$

Χρησιμοποιώντας τη στοιχειώδη ανισότητα $n!/(\lfloor n/2\rfloor!)^2\leqslant 2(n+1)^{1/2}2^n$ και με απλούς υπολογισμούς βλέπουμε ότι το εσωτερικό άθροισμα φράσσεται από $2^{4m}((m-t_1)!(m-t_2)!)^{-1/2}$ και έπεται το ζητούμενο. □

Το τελευταίο λήμμα αυτής της ενότητας δίνει μια σχέση ανάμεσα στην κάλυψη και την διάσταση.

Λήμμα 3.3.3. *Έστω $\Gamma \subset \widehat{G}$ ένα συμμετρικό σύνολο. Αν το $\Delta \subset \widehat{G}$ έχει Γ-διάσταση r τότε υπάρχει διαμέριση $\widehat{G} = \Lambda_0 \bigsqcup \Lambda_1$ όπου το Λ_0 έχει $2r$-κάλυψη από το Γ και για κάθε $\gamma \in \Lambda_1$ το σύνολο $\Delta \cup \{\gamma\}$ έχει Γ-διάσταση $r+1$.*

Απόδειξη. Από την υπόθεση μπορούμε να γράψουμε $\Delta = \Delta_0 \bigsqcup \Delta_1$ όπου το Δ_0 είναι Γ-αποσυνδεδεμένο και $|\Delta_1| = r$. Έστω Δ' το σύνολο όλων των $\gamma \in \widehat{G}$ για τα οποία το $\Delta_0 \cup \{\gamma\}$ δεν είναι Γ-αποσυνδεδεμένο. Θα δείξουμε ότι η διάσπαση $\Lambda_0 = \Delta' \cup \Delta_0$ και $\Lambda_1 = \widehat{G} \setminus \Lambda_0$ ικανοποιεί το ζητούμενο.

Έστω $\gamma \in \Lambda_1$. Από την κατασκευή, το σύνολο $\Delta_0 \cup \{\gamma\}$ είναι Γ-αποσυνδεδεμένο, άρα το $\Delta \cup \{\gamma\}$ έχει Γ-διάσταση μεγαλύτερη ή ίση από $r+1$ από τον ορισμό, αφού $|\Delta_0 \cup \{\gamma\}| = r+1$. Μένει να δείξουμε ότι το Λ_0 έχει $2r$-κάλυψη από το Γ. Για το σκοπό αυτό, αρκεί να δείξουμε ότι

$$\Delta_0 \cup \Delta' \subset \Gamma - \Gamma + \langle \Delta_0 \rangle + \langle \Delta_0 \rangle.$$

Αυτό είναι φανερό για το Δ_0. Έστω $\gamma \in \Delta'$. Από την κατασκευή, το $\Delta_0 \cup \{\gamma\}$ δεν είναι Γ-αποσυνδεδεμένο, άρα υπάρχουν $k \geqslant 1$ και $\lambda \in \widehat{G}$ τέτοια ώστε να υπάρχουν περισσότερες από 2^k τριάδες $(\varepsilon, \Delta_1', \Delta_2')$ ώστε $\varepsilon \in \{-1, 0, 1\}$, τα σύνολα Δ_1' και Δ_2' είναι ξένα υποσύνολα του Δ_0 με $|\Delta_1' \cup \Delta_2'| + |\varepsilon| = k$, και

$$\varepsilon\gamma + \sum_{\gamma_1' \in \Delta_1'} \gamma_1' - \sum_{\gamma_2' \in \Delta_2'} \gamma_2' \in \Gamma + \lambda.$$

Αν υπάρχει τουλάχιστον μία τέτοια τριάδα με $\varepsilon = 0$ και τουλάχιστον μία με $\varepsilon \neq 0$ τότε είναι εύκολο να ελέγξουμε ότι $\gamma \in \Gamma - \Gamma + \langle \Delta_0 \rangle - \langle \Delta_0 \rangle$ όπως θέλουμε. Αν $\varepsilon = 0$ για όλες αυτές τις τριάδες τότε καταλήγουμε σε άτοπο αφού το Δ_0 είναι Γ-αποσυνδεδεμένο. Μπορούμε λοιπόν να υποθέσουμε ότι $\varepsilon \in \{-1, 1\}$ για όλες αυτές τις τριάδες. Αυτό δεν μπορεί φυσικά να συμβεί αν $k = 1$, και αν $k > 1$ παρατηρούμε ότι από την αρχή του περιστερώνα υπάρχουν περισσότερες από 2^{k-1} τέτοιες τριάδες που έχουν όλες το ίδιο ε. Αυτό όμως οδηγεί πάλι σε αντίφαση αφού το Δ_0 είναι Γ-αποσυνδεδεμένο, αν θεωρήσουμε τη μεταφορά $\Gamma + \lambda - \varepsilon\gamma$. Άρα, $\gamma \in \Gamma - \Gamma + \langle \Delta_0 \rangle - \langle \Delta_0 \rangle$ όπως θέλαμε, και η απόδειξη είναι πλήρης. □

Το επόμενο θεώρημα αποδεικνύεται με την πιθανοθεωρητική μέθοδο και μας εξασφαλίζει ότι αν ένα σύνολο έχει την ιδιότητα ότι κάθε μεγάλο υποσύνολό του δεν καλύπτεται αποτελεσματικά τότε πρέπει να έχει ιδιαίτερα μικρή προσθετική ενέργεια. Το επιχείρημα που χρησιμοποιούμε έχει πολλές ομοιότητες με προηγούμενο επιχείρημα των Bateman και Katz. Χρειαζόμαστε όμως μια εκδοχή του για την $2m$-πλή προσθετική ενέργεια με το $m \to \infty$ όταν το $N \to \infty$ (συγκεκριμένα θα χρειαστεί να επιλέξουμε $m \approx (\log\log N)^{1+o(1)}$) οπότε πρέπει να γίνει σαφής η εξάρτηση από το m.

Θεώρημα 3.3.4. *Έστω $\Gamma \subset \widehat{G}$ συμμετρικό σύνολο και $\omega : \widehat{G} \to \mathbb{R}^+$. Έστω $m \geqslant 2$ και $d \geqslant n \geqslant 2$ τέτοιοι ώστε $m \leqslant d/4$ και $\|\omega\|_2 \leqslant \sqrt{m} d^{-1} \|\omega\|_1$. Τότε, είτε υπάρχει πεπερασμένο* *σύνολο* $\Delta \subset \widehat{G}$ *τέτοιο ώστε το* Δ *να έχει* $2d$*-κάλυψη από το* Γ *και*

$$\sum_{\gamma \in \Delta} \omega(\gamma) \geqslant \frac{n}{d}\|\omega\|_1$$

ή

$$E_{2n}(\omega, \Gamma) \leqslant 2^{13m+6n} m^{2m} d^{-2m} \|\omega\|_1^{2m}.$$

Απόδειξη. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\|\omega\|_1 = 1$. Παρατηρούμε αρχικά ότι είτε βρισκόμαστε στην πρώτη περίπτωση ή κάθε υποσύνολο $\Delta \subset \widehat{G}$ το οποίο έχει $2d$-κάλυψη από το Γ ικανοποιεί την

$$\sum_{\gamma \in \Delta} \omega(\gamma) \leqslant n/d,$$

οπότε κάνουμε αυτή την υπόθεση από εδώ και πέρα.

Έστω $S \subset \widehat{G}$ τυχαίο σύνολο με πληθάριθμο το πολύ d, το οποίο ορίζεται αν πάρουμε d στοιχεία του $\widehat{G}$ τυχαία, επιλέγοντας το $\gamma \in \widehat{G}$ με πιθανότητα $\omega(\gamma)$. Θα δείξουμε ότι για κάθε $k \geqslant 0$ το σύνολο S έχει Γ-διάσταση $d-k$ με πιθανότητα μικρότερη ή ίση από $n^k/k!$.

Πράγματι, έστω ότι έχουμε επιλέξει $d' \leqslant d$ στοιχεία του S, που σχηματίζουν ένα σύνολο S', και έστω ότι το S' έχει Γ-διάσταση r. Από το Λήμμα 3.3.3 μπορούμε να βρούμε διαμέριση $\widehat{G} = \Lambda \bigsqcup \Lambda_1$ τέτοια ώστε το Λ_0 να έχει $2d$-κάλυψη από το Γ και για κάθε $\gamma \in \Lambda_1$ το σύνολο $S' \cup \{\gamma\}$ να έχει Γ-διάσταση τουλάχιστον $r+1$. Συνεπώς,

$$\mathbb{P}(\dim(S' \cup \{\gamma\}) \leqslant \dim(S')) \leqslant \sum_{\gamma \in \Lambda_0} \omega(\gamma) \leqslant \frac{n}{d},$$

αφού το Λ_0 έχει $2d$-κάλυψη από το Γ.

Έστω $1 \leqslant k \leqslant 2m$. Για οποιαδήποτε διακεκριμένα $\gamma_1, \ldots, \gamma_k \in \widehat{G}$ η πιθανότητα να ισχύει ότι $\gamma_1, \ldots, \gamma_k \in S$ είναι τουλάχιστον

$$k!\binom{d}{k}\omega(\gamma_1)\cdots\omega(\gamma_k)\left(1 - \sum_{i=1}^{k}\omega(\gamma_i)\right)^{d-k}.$$

Αφού $k \leqslant d/2$, έχουμε $k!\binom{d}{k} \geqslant (d/2)^k$. Επιπλέον, από την ανισότητα Cauchy-Schwarz,

$$\sum_{i=1}^{k}\omega(\gamma_i) \leqslant \sqrt{2m}\|\omega\|_2 \leqslant 2m/d \leqslant 1/2,$$

άρα ο τελευταίος παράγοντας είναι τουλάχιστον

$$\exp\left(-d\sum_{i=1}^{k}\omega(\gamma_i)\right) \geqslant e^{-2m}.$$

Έπεται ότι η πιθανότητα να ισχύει ότι $\gamma_1, \ldots, \gamma_k \in S$ είναι τουλάχιστον

$$2^{-5m} d^k \omega(\gamma_1) \cdots \omega(\gamma_k).$$

Από τη γραμμικότητα της μέσης τιμής, υποθέτοντας ότι $t_1 + t_2 \leqslant m$, έχουμε

$$\mathbb{E}\, E^{\#}_{t_1,t_2}(S, \Gamma + \lambda) \geqslant 2^{-5m} d^{t_1+t_2} E^{\#}_{t_1,t_2}(\omega, \Gamma + \lambda),$$

άρα, για κάθε $\lambda \in \widehat{G}$ και $0 \leqslant t_1, t_2 \leqslant m$,

$$E^{\#}_{t_1,t_2}(\omega, \Gamma + \lambda) \leqslant 2^{7m} e^{4n} d^{-t_1-t_2}.$$

Από το Λήμμα 3.3.2 έπεται ότι

$$E_{2m}(\omega, \Gamma) \leqslant 2^{11m} e^{4n} m! \|\omega\|_2^{2m} \left(\sum_{0 \leqslant t \leqslant m} \frac{(m!)^{1/2} (\|\omega\|_2^{-1} d^{-1})^t}{((m-1)!)^{1/2}} \right)^2.$$

Ορίζουμε $r := \|\omega\|_2^{-2} d^{-2} \geqslant m^{-1}$. Από την ανισότητα Cauchy-Schwarz, ο όρος μέσα στην παρένθεση είναι το πολύ ίσος με

$$(m+1) \sum_{0 \leqslant t \leqslant m} \frac{m!}{(m-t)!} r^t \leqslant (m+1) \sum_{0 \leqslant t \leqslant m} (erm)^t \leqslant (m+1)^2 (erm)^m.$$

Ειδικότερα,

$$E_{2m}(\omega, \Gamma) \leqslant 2^{13m} e^{4n} m^{2m} \|\omega\|_2^{2m} r^m = 2^{13m} e^{4n} m^{2m} d^{-2m},$$

και έπεται το ζητούμενο. □

3.4 Δομή του φάσματος

Τα αποτελέσματα της προηγούμενης ενότητας είναι πολύ γενικά και μπορούμε να τα χρησιμοποιήσουμε για να πάρουμε συμπεράσματα για τη διάσταση οποιουδήποτε συνόλου αν διαθέτουμε κάτω φράγμα για την προσθετική του ενέργεια. Χρησιμοποιώντας τα θα αποδείξουμε ένα θεώρημα δομής για το μεγάλο φάσμα μιας συνάρτησης $f : G \to \mathbb{C}$ και για το σκοπό αυτό χρειαζόμαστε κάποιο κάτω φράγμα για την προσθετική ενέργεια ενός τέτοιου φάσματος. Ένα κατάλληλο κάτω φράγμα έχει δοθεί από τον Shkredov, ο οποίος απέδειξε ότι αν $A \subset G$ είναι ένα σύνολο με πυκνότητα $\alpha = |A|/N$ και αν $\Delta \subset \Delta_\eta(A)$ τότε

$$E_{2m}(\Delta, \{0\}) \gg \eta^{2m} \alpha |\Delta|^{2m}.$$

Το επόμενο λήμμα γενικεύει το αποτέλεσμα (και το επιχείρημα) του Shkredov.

Λήμμα 3.4.1. *Έστω $\varepsilon \in [0,1]$. Έστω $B \subset G$ και $\eta \in [0,1]$ και έστω $f : B \to \mathbb{C}$ και $\omega : \widehat{G} \to \mathbb{R}^+$. Τότε, για κάθε ακέραιο $m \geqslant 1$,*

$$E_{2m}(\omega, \Delta_\varepsilon(B)) \geqslant \|\omega\|_1^{2m} \left(\left(\eta \frac{\|f\|_1}{\|f\|_{2m/(2m-1)}|B|^{1/2m}} \right)^{2m} - \varepsilon \right).$$

Απόδειξη. Ορίζουμε χ μέσω της $\widehat{\chi}(\gamma) = \overline{c_\gamma}\omega(\gamma)$, όπου $c_\gamma \widehat{f}(\gamma) = |\widehat{f}(\gamma)|$. Από την κατασκευή, αν $\omega(\gamma) \neq 0$ τότε $|\widehat{f}(\gamma)| \geqslant \eta\|f\|_1$, συνεπώς

$$\sum_x f(x)\overline{\chi(x)} = \frac{1}{N}\sum_\gamma \widehat{f}(\gamma)\overline{\widehat{\chi}(\gamma)} = \frac{1}{N}\sum_\gamma \omega(\gamma)|\widehat{f}(\gamma)| \geqslant \frac{1}{N}\eta\|f\|_1\|\omega\|_1.$$

Από την ανισότητα Hölder έχουμε

$$\left(\sum_x f(x)\overline{\chi(x)}\right)^{2m} \leqslant \left(\sum_x |f(x)|^{2m/(2m-1)}\right)^{2m-1} \left(\sum_x B(x)|\chi(x)|^{2m}\right).$$

Παρατηρούμε τώρα ότι, από την τριγωνική ανισότητα,

$$\begin{aligned}\sum_x B(x)|\chi(x)|^{2m} &= \frac{1}{N^{2m}}\sum_x B(x)\left|\sum_\gamma c_\gamma(\omega)\omega(\gamma)\gamma(x)\right|^{2m} \\ &\leqslant \frac{1}{N^{2m}} \sum_{\gamma_1,\ldots,\gamma_m'} \omega(\gamma_1)\cdots\omega(\gamma_m')|\widehat{B}(\gamma_1+\cdots-\gamma_m')|.\end{aligned}$$

Έπεται ότι

$$\begin{aligned}\eta^{2m}\|f\|_1^{2m}\|\omega\|_1^{2m} &\leqslant \|f\|_{2m/(2m-1)}^{2m} \sum_{\gamma_1,\ldots,\gamma_m'} \omega(\gamma_1)\cdots\omega(\gamma_m')|\widehat{B}(\gamma_1+\cdots-\gamma_m')| \\ &\leqslant \|f\|_{2m/(2m-1)}^{2m}\Big(|B|E_{2m}(\omega,\Delta_\varepsilon(B)) + \varepsilon|B|\,\|\omega\|_1^{2m}\Big).\end{aligned}$$

Αυτό ολοκληρώνει την απόδειξη. □

Το φράγμα του Shkredov προκύπτει από το Λήμμα 3.4.1 αν θέσουμε $B = G$ και αφήσουμε το $\varepsilon \to 0$. Μπορούμε τώρα να αποδείξουμε το κεντρικό τεχνικό αποτέλεσμα του Bloom, το οποίο θα παίξει το ρόλο του λήμματος της Chang. Για τις εφαρμογές θα χρειαστούμε μια αρκετά γενική εκδοχή του, ο αναγνώστης θα μπορούσε όμως αρχικά να θεωρήσει την ειδική περίπτωση $B = G$ και $\varepsilon > 0$, οπότε $\Delta_\varepsilon(B) = \{0\}$.

Θεώρημα 3.4.2. *Έστω $f : B \to \mathbb{C}$ και $\alpha = \|f\|_1/\|f\|_\infty|B|$. Θεωρούμε $\omega : \widehat{G} \to \mathbb{R}^+$ με φορέα στο $\Delta_\eta(f)$ και $0 \leqslant \varepsilon \leqslant \exp(-8\mathcal{L}(\eta)\mathcal{L}(\alpha))$. Υπάρχει $\Delta' \subset \Delta_\eta(f)$ το οποίο έχει $2^{14}\mathcal{L}(\alpha)\eta^{-1}$-κάλυψη από το $\Delta_\varepsilon(B)$ τέτοιο ώστε*

$$\sum_{\gamma\in\Delta'}\omega(\gamma) \geqslant 2^{-12}\eta\|\omega\|_1.$$

Απόδειξη. Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $\|\omega\|_1 = 1$. Υποθέτουμε αρχικά ότι $\|\omega\|_2 \geqslant 2^{-12}\mathcal{L}(\alpha)^{-1/2}\eta$ και θεωρούμε το τυχαίο σύνολο Δ' που προκύπτει αν συμπεριλάβουμε σε αυτό το $\gamma \in \widehat{G}$ με πιθανότητα $2^{13}\eta^{-1}\mathcal{L}(\alpha)\omega(\gamma)$. Από την ανισότητα Chernoff έχουμε $|\Delta'| \leqslant 2^{14}\eta^{-1}\mathcal{L}(\alpha)$ με πιθανότητα τουλάχιστον 7/8 και

$$\mathbb{E}\left(\sum_{\gamma\in\Delta'}\omega(\gamma)\right) \geqslant 2^{13}\eta^{-1}\mathcal{L}(\alpha)\|\omega\|_2^2 \geqslant 2^{-11}\eta,$$

άρα από την ανισότητα Markov έχουμε $\sum_{\gamma\in\Delta'}\omega(\gamma) \geqslant 2^{-12}\eta$ με πιθανότητα μεγαλύτερη από 1/2 και έπεται ο ισχυρισμός του θεωρήματος.

Αλλιώς, θέτουμε $n = m = \mathcal{L}(\alpha)$ και $d = \lfloor 2^{12}\eta^{-1}m\rfloor$ και εφαρμόζουμε τα Λήμματα 3.4.1 και 3.3.1. Από τα προηγούμενα μπορούμε να υποθέσουμε ότι $\|\omega\|_2 \leqslant 2^{-12}\mathcal{L}(\alpha)^{-1/2}\eta \leqslant m^{1/2}/d$, όπως απαιτείται για να εφαρμόσουμε το Λήμμα 3.3.1. Από το Λήμμα 3.4.1 έπεται ότι

$$E_{2m}(\omega;\Delta_\varepsilon(B)) \geqslant \left(\eta\frac{\|f\|_1}{\|f\|_{2m/(2m-1)}|B|^{1/2m}}\right)^{2m} - \varepsilon.$$

Έχουμε το τετριμμένο φράγμα $\|f\|_{2m/(2m-1)} \leqslant \|f\|_\infty^{1/2m}\|f\|_1^{1-1/2m}$, άρα αν $\varepsilon \leqslant \eta^{2m}\alpha/2$ τότε

$$E_{2m}(\omega;\Delta_\varepsilon(B)) \geqslant \eta^{2m}\alpha/2.$$

Από το Λήμμα 3.3.1 είτε υπάρχει κάποιο σύνολο Δ' το οποίο έχει $2d$-κάλυψη από το $\Delta_\varepsilon(B)$ τέτοιο ώστε

$$\sum_{\gamma\in\Delta'}\omega(\gamma) \geqslant \frac{m}{d}$$

ή

$$\eta^{2m}\alpha \leqslant 2^{19m+1}m^{2m}d^{-2m}.$$

Ειδικότερα,

$$d \leqslant 2^{10}m\eta^{-1}\alpha^{-1/2m},$$

και αυτό έρχεται σε αντίθεση με την αρχική επιλογή των d και m, άρα η απόδειξη είναι πλήρης. □

Το Θεώρημα 3.1.6 είναι ειδική περίπτωση του Θεωρήματος 3.4.2. Προκύπτει από αυτό αν επιλέξουμε $B = G$, αφήσουμε το $\varepsilon \to 0$ και πάρουμε σαν ω την δείκτρια συνάρτηση του $\Delta_\eta(f)$.

3.5 Αύξηση της πυκνότητας

Λήμμα 3.5.1. *Έστω $f : B \to [0,1]$ και $g = f - \alpha B$, όπου $\alpha = \|f\|_1/B$. Υποθέτουμε ότι*

$$\sum_{\gamma\in\Gamma} |\widehat{g}(\gamma)|^2 \geqslant \nu\alpha\|f\|_1 N.$$

Τότε, αν B' είναι ένα συμμετρικό σύνολο τέτοιο ώστε για κάθε $\gamma \in \Gamma$ να ισχύει

$$|\widehat{B'}(\gamma| \geqslant 2^{-1}|B|$$

και επιπλέον $|(2B' + B) \setminus B| \leqslant 2^{-4}\nu\alpha|B|$, τότε

$$\|f * B'\|_\infty \geqslant (1 + 2^{-3}\nu)\alpha|B'|.$$

Απόδειξη. Από την υπόθεση έχουμε

$$\sum_{\gamma} |\widehat{g}(\gamma)|^2|\widehat{B'}(\gamma)|^2 \geqslant 2^{-2}\nu\alpha\|f\|_1|B'|^2 N.$$

Ειδικότερα,

$$\|g * B'\|_2^2 = \frac{1}{N}\sum_{\gamma} |\widehat{g}(\gamma)|^2|\widehat{B'}(\gamma)|^2 \geqslant 2^{-2}\nu\alpha\|f\|_1|B'|^2.$$

Αναπτύσσοντας την L^2-νόρμα παίρνουμε

$$\sum_{x} |f * B'(x)|^2 + \alpha^2\|B * B'\|_2^2 - 2\alpha\langle B * B', f * B'\rangle \geqslant 2^{-2}\nu\alpha\|f\|_1|B'|^2.$$

Από την υπόθεση,

$$\begin{aligned}\Big|\langle B * B', f * B'\rangle - \|f\|_1|B'|^2\Big| &\leqslant |B'|^2 \sup_{x,y\in B'} \sum_{x\notin B} f(z + x - y)\\ &\leqslant |B'|^2|(2B' + B) \setminus B|\\ &\leqslant 2^{-4}\nu\|f\|_1|B'|^2.\end{aligned}$$

Έπεται ότι

$$\|f * B'\|_2^2 \geqslant (1 + 2^{-3}\nu)\alpha\|f\|_1|B'|^2.$$

Το αριστερό μέλος φράσσεται από $\|f\|_1|B'|\,\|f * B'\|\infty$, και έπεται το λήμμα. □

Το δεύτερο λήμμα δείχνει ότι αν ένα σύνολο έχει μικρή διάσταση τότε από τον έλεγχο σε λίγα στοιχεία μπορούμε να πάρουμε έλεγχο σε ολόκληρο το σύνολο.

Λήμμα 3.5.2. *Αν το $\Delta \subset \widehat{G}$ έχει d-κάλυψη από το Γ τότε υπάρχει $\Lambda \subset \widehat{G}$ με πληθάριθμο το πολύ ίσο με d τέτοιο ώστε αν το B έχει $(4d)^{-1}$-έλεγχο των Λ και $\Gamma(1/8)$ τότε για κάθε $\gamma \in \Delta$ ισχύει*

$$|\widehat{B}(\gamma)| \geqslant 2^{-1}|B|.$$

Απόδειξη. Από την υπόθεση υπάρχει κάποιο $\Lambda \subset \widehat{G}$ τέτοιο ώστε $|\Lambda| \leqslant d$ και

$$\Delta \subset \Gamma - \Gamma + \langle \Lambda \rangle.$$

Έστω $\gamma \in \Delta$. Τότε υπάρχουν $\gamma_0, \gamma_1 \in \Gamma$ και $\varepsilon \in \{-1, 0, 1\}^{\Lambda}$ τέτοια ώστε

$$\gamma = \gamma_0 - \gamma_1 + \sum_{\lambda \in \Lambda} \varepsilon_\lambda \lambda.$$

Από την τριγωνική ανισότητα, για κάθε $x \in B$ έχουμε

$$|1 - \gamma(x)| \leqslant |1 - \gamma_0(x)| + |1 - \gamma_1(x)| + d \sup_{\lambda \in \Lambda} |1 - \lambda(x)| \leqslant 1/2.$$

Έπεται ότι

$$\left| \widehat{B}(\gamma) - |B| \right| \leqslant \sum_{x \in B} |1 - \gamma(x)| \leqslant 2^{-1}|B|$$

και έπεται το συμπέρασμα. □

Τέλος, έχοντας υπόψη μας το Θεώρημα 3.4.2 βλέπουμε ότι για να χρησιμοποιήσουμε το Λήμμα 3.5.2 θα χρειαστούμε να έχουμε καλό έλεγχο στο φάσμα δοθέντος συνόλου. Το επόμενο λήμμα μας δίνει ένα πιο χρήσιμο κριτήριο που μας το εξασφαλίζει.

Λήμμα 3.5.3. *Αν $c > 0$ και $|(B + B') \setminus B| \leqslant c\varepsilon|B|$ τότε το B' έχει $2c$-έλεγχο του $\Delta_\varepsilon(B)$.*

Απόδειξη. Επιλέγουμε γ τέτοιο ώστε $|\widehat{B}(\gamma)| \geqslant \varepsilon|B|$ και $x \in B'$. Τότε

$$\begin{aligned} |1 - \gamma(x)|\,|B| &\leqslant \varepsilon^{-1} \left| \sum_{y \in B} \gamma(y) - \sum_{y \in B + x} \gamma(y) \right| \\ &\leqslant 2\varepsilon^{-1} |(B + B') \setminus B| \\ &\leqslant 2c|B|. \end{aligned}$$

□

Συνδυάζοντας όλα αυτά τα εργαλεία μπορούμε να αποδείξουμε το επόμενο αποτελεσματικό θεώρημα αύξησης της πυκνότητας.

Θεώρημα 3.5.4. *Έστω* $B, B' \subset G$. *Έστω* $A \subset B$ *με πυκνότητα* $\alpha = |A|/|B|$ *και* $f : B' \to [-1, 1]$ *με πυκνότητα* $\tau = \|f\|_1/|B|$. *Ορίζουμε* $D(x) = A(x) - \alpha B(x)$ *και υποθέτουμε ότι*

$$\sum_{\gamma} |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2 = \nu\alpha\|f\|_1|A|\,N.$$

Τότε υπάρχει πεπερασμένο σύνολο $\Lambda \subset \widehat{G}$ *με πληθάριθμο*

$$d = |\Lambda| \leqslant 2^{16}\mathcal{L}(\tau)(\nu\alpha)^{-1}$$

τέτοιο ώστε αν ένα συμμετρικό σύνολο $B'' \subset G$ *έχει* $(4d)^{-1}$*-έλεγχο του* Λ,

$$|(2B'' + B) \setminus B| \leqslant 2^{-17}\nu\alpha|B|,$$

και

$$|(B'' + B') \setminus B'| \leqslant 2^{-4}\exp(-2^4\mathcal{L}(\tau)\mathcal{L}(\nu\alpha))|B'|,$$

τότε υπάρχει x *τέτοιο ώστε*

$$|(A - x) \cap B''| \geqslant (1 + 2^{-16}\nu)\alpha|B''|.$$

Απόδειξη. Θέτουμε $\Delta = \Delta_\eta(f)$ όπου $\eta = \nu\alpha/2$. Ειδικότερα,

$$\sum_{\gamma\notin\Delta} |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2 \leqslant 2^{-1}\nu\alpha\|f\|_1\|D\|_2^2 N \leqslant 2^{-1}\nu\alpha\|f\|_1|A|\,N.$$

Ειδικότερα,

$$\sum_{\gamma\in\Delta} |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2 \geqslant 2^{-1}\nu\alpha\|f\|_1|A|\,N.$$

Τώρα θεωρούμε μια δυαδική διαμέριση του Δ στα σύνολα $\Delta_i = \Delta_{2^i\eta}(f)$, και εφαρμόζουμε το Θεώρημα 3.4.2 για κάθε Δ_i με τη συνάρτηση βάρους

$$\omega(\gamma) = |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2$$

και

$$\varepsilon = \exp(-2^4\mathcal{L}(\nu\alpha)\mathcal{L}(\tau)) \leqslant \exp(-8\mathcal{L}(\eta)\mathcal{L}(\tau)).$$

Τότε, αν Δ_i' είναι το σύνολο που μας δίνει το Θεώρημα 3.4.2, έχουμε

$$\begin{aligned} 2^{-12}\sum_{\gamma\in\Delta_i} |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2 &\leqslant (2^i\eta)^{-1}\sum_{\gamma\in\Delta_i'} |\widehat{f}(\gamma)|\,|\widehat{D}(\gamma)|^2 \\ &\leqslant 2\|f\|_1\sum_{\gamma\in\Delta_i'} |\widehat{D}(\gamma)|^2. \end{aligned}$$

Αθροίζοντας πάνω από όλα τα $i \geqslant 0$ βλέπουμε ότι

$$\sum_{\gamma \in \Delta'} |\widehat{D}(\gamma)|^2 = \sum_i \sum_{\gamma \in \Delta'_i} |\widehat{D}(\gamma)|^3 \geqslant 2^{-13} \nu\alpha |A| N,$$

όπου $\Delta' = \bigcup_{i \geqslant 0} \Delta'_i$. Αφού κάθε Δ'_i έχει $2^{14}\mathcal{L}(\tau)(2^i\eta)^{-1}$-κάλυψη από το $\Delta_\varepsilon(B')$ έπεται ότι το Δ' έχει d-κάλυψη από το $\Delta_\varepsilon(B')$ με

$$d \leqslant 2^{14}\mathcal{L}(\tau) \sum_i (2^i\eta)^{-1} \leqslant 2^{16}\mathcal{L}(\tau)(\nu\alpha)^{-1}.$$

Αφού το B'' ικανοποιεί την $|(B''+B') \setminus B'| \leqslant 2^{-4}\varepsilon|B'|$, έπεται από το Λήμμα 3.5.3 ότι το B'' έχει 2^{-3}-έλεγχο του $\Delta_\varepsilon(B')$. Από το Λήμμα 3.5.2 βλέπουμε ότι υπάρχει κάποιο Λ με πληθάριθμο $d \leqslant 2^{16}\mathcal{L}(\tau)(\nu\alpha)^{-1}$ τέτοιο ώστε αν το B'' έχει $(4d)^{-1}$-έλεγχο του Λ τότε για κάθε $\gamma \in \Delta'$ ισχύει

$$|\widehat{B''}(\gamma)| \geqslant 2^{-1}|B''|.$$

Αφού έχουμε επίσης $|(2B''+B) \setminus B| \leqslant 2^{-17}\nu\alpha|B|$, από το Λήμμα 3.5.1 έπεται ότι

$$|(A-x) \cap B''| \geqslant (1+2^{-16}\nu)\alpha|B''|$$

όπως θέλαμε. □

Στόχος μας ήταν να μελετήσουμε το πλήθος των λύσεων της (3.1.1) σε ένα δοθέν σύνολο A. Ο αριθμός αυτός είναι ίσος με $\langle (c_1 \cdot A) * (c_2 \cdot A), (-c_3 \cdot A)\rangle$. Χρησιμοποιώντας την ταυτότητα Parseval και το Θεώρημα 3.5.4 μπορούμε να αποδείξουμε το επόμενο γενικό θεώρημα αύξησης της πυκνότητας, το οποίο δείχνει ότι είτε αυτός ο αριθμός είναι μεγάλος ή κάποιο πολλαπλάσιο του A έχει αυξημένη πυκνότητα σε κάποιο δομημένο υποσύνολο.

Θεώρημα 3.5.5. *Έστω $B' \subset B \subset G$ και έστω $A_1 \subset B'$ και $A_2, A_3 \subset B$ με σχετικές πυκνότητες α_i. Θέτουμε $\alpha = 2^{-1}\min(2^{-5}, \alpha_1, \alpha_2, \alpha_3)$ και υποθέτουμε ότι*

$$|(B'+B) \setminus B| \leqslant 2^{-2}\alpha|B|.$$

Τότε, είτε

$$\langle A_1 * A_2, A_3 \rangle \geqslant 2^{-2}\alpha_1\alpha_2\alpha_3|B|\,|B'| \tag{3.5.1}$$

ή υπάρχει πεπερασμένο σύνολο $\Lambda \subset \widehat{G}$ με πληθάριθμο

$$d = |\Lambda| \leqslant 2^{10}\mathcal{L}(\alpha)\alpha^{-1}$$

τέτοιο ώστε αν ένα συμμετρικό σύνολο B'' έχει $(4d)^{-1}$-έλεγχο του Λ,

$$|(2B''+B) \setminus B| \leqslant 2^{-19}\alpha|B|$$

και

$$|(B'' + B') \setminus B'| \leqslant 2^{-4} \exp(-2^5 \mathcal{L}(\alpha)^2)|B'|$$

τότε υπάρχουν $x \in G$ *και* $i \in \{2,3\}$ *τέτοια ώστε*

$$|(A_i - x) \cap B''| \geqslant (1 + 2^{-18})\alpha_i |B''|.$$

Απόδειξη. Ορίζουμε $D_i = A_i - \alpha_i B$ για $i = 2,3$ και $D_1 = A_1 - \alpha_1 B'$. Έχουμε

$$\begin{aligned}\sum_x A_1 * D_2(x) D_3(x) = \sum_x A_1 * A_2(x) A_3(x) - \alpha_2 \sum_{x \in B} A_3 * A_1^-(x) \\ - \alpha_3 \sum_{x \in B} A_1 * A_2(x) + \alpha_2 \alpha_3 \sum_{x \in B} B * A_1(x).\end{aligned}$$

Παρατηρούμε ότι αν το A' έχει φορέα στο B' και το A έχει φορέα στο B τότε

$$\left| \sum_{x \in B} A' * A(x) - |A'|\,|A| \right| \leqslant |A'|\,|(B' + B) \setminus B| \leqslant 2^{-2} |A'|\,|A|.$$

Ειδικότερα,

$$\sum_x A_1 * D_2(x) D_3(x) \leqslant \sum_x A_1 * A_2(x) A_3(x) - 2^{-1} \alpha_1 \alpha_2 \alpha_3 |B|\,|B'|.$$

Από την τριγωνική ανισότητα είτε ισχύει η (3.5.1) ή

$$\sum_\gamma |\widehat{A_1}(\gamma)|\,|\widehat{D_2}(\gamma)|\,|\widehat{D_3}(\gamma)| \geqslant 2^{-2} \alpha_1 \alpha_2 \alpha_3 |B|\,|B'|\,N.$$

Εφαρμόζοντας την ανισότητα Cauchy-Schwarz παίρνουμε

$$\left(\sum_\gamma |\widehat{A_1}(\gamma)|\,|\widehat{D_2}(\gamma)|^2 \right) \left(\sum_\gamma |\widehat{A_1}(\gamma)|\,|\widehat{D_3}(\gamma)|^2 \right) \geqslant 2^{-4} |A_1|^2 \alpha_2^2 \alpha_3^2 |B|^2 N^2.$$

Έπεται ότι για κάποιο $i \in \{2,3\}$ έχουμε

$$\sum_\gamma |\widehat{A_1}(\gamma)|\,|\widehat{D_i}(\gamma)|^2 \geqslant 2^{-2} |A_1| \alpha_i^2 |B| N,$$

και το ζητούμενο προκύπτει από το Θεώρημα 3.5.4. □

3.6 Πολυωνυμικοί δακτύλιοι

Για την πρώτη εφαρμογή της μεθόδου που περιγράψαμε, επιλέγουμε $G = \mathbb{F}_q[t]/(p(t))$, όπου $p(t)$ κάποιος πρώτος βαθμού n, οπότε $N = q^n$, και q είναι κάποια περιττή δύναμη πρώτου. Συμβολίζουμε αυτή την ομάδα με $\mathcal{U}_N$. Αυτή η ομάδα είναι αρκετά πλούσια ώστε να έχει αρκετές ομοιότητες με τους ακεραίους, ενώ ταυτόχρονα έχει το σημαντικό τεχνικό πλεονέκτημα της πεπερασμένης χαρακτηριστικής.

Σταθεροποιούμε κάποιους συντελεστές $c_1, c_2, c_3 \in \mathbb{F}_q[t] \setminus \{0\}$ με $c_1 + c_2 + c_3 = 0$, και ένα πεπερασμένο σύνολο $A \subseteq \mathcal{U}_N$. Υποθέτουμε ότι ο N είναι αρκετά μεγάλος ώστε αυτοί οι συντελεστές να είναι πρώτοι προς το $p(t)$. Θέλουμε να μελετήσουμε τη συνάρτηση που μετράει το πλήθος των λύσεων της $c_1x_1 + c_2x_2 + c_3x_3 = 0$ με $x_i \in A$, την οποία συμβολίζουμε με

$$\Upsilon_{\mathbf{c}}(A) = \langle (c_1 \cdot A) * (c_2 \cdot A), (-c_3 \cdot A) \rangle. \tag{3.6.1}$$

Παρατηρούμε ότι η $\Upsilon_{\mathbf{c}}(A)$ είναι αναλλοίωτη ως προς διαστολές και μεταφορές του A.

Οι $\mathcal{U}_N$ και $\widehat{\mathcal{U}_N}$ είναι $\mathbb{F}_q$-διανυσματικοί χώροι διάστασης n. Επιπλέον, κάθε $a \in \mathcal{U}_N$ δρα στην $\widehat{\mathcal{U}_N}$ μέσω της $(a\gamma)(x) = \gamma(ax)$. Ο χώρος Bohr της $\Gamma \subset \widehat{\mathcal{U}_N}$ ορίζεται από την

$$B(\Gamma) = \{x \in \mathcal{U}_N : \gamma(x) = 1 \text{ για κάθε } \gamma \in \Gamma\}.$$

Αν B είναι ένας χώρος Bohr τότε το σύνολο συχνοτήτων του B είναι το

$$[B] = \{\gamma \in \widehat{\mathcal{U}_N} : \gamma(x) = 1 \text{ για κάθε } x \in B\},$$

και ορίζουμε την τάξη του B να είναι η $\mathbb{F}_q$-διάσταση του $[B]$.

Λήμμα 3.6.1. *Κάθε χώρος Bohr είναι $\mathbb{F}_q$-υπόχωρος του $\mathcal{U}_N$, και αντίστροφα, κάθε $\mathbb{F}_q$-υπόχωρος του $\mathcal{U}_N$ είναι χώρος Bohr. Επιπλέον, αν το B είναι χώρος Bohr τότε*

$$|B| = q^{-\mathrm{rk}(B)} N. \tag{3.6.2}$$

Απόδειξη. Δείχνουμε αρχικά ότι αν V είναι ένας $\mathbb{F}_q$-υπόχωρος του $\mathcal{U}_N$ τότε $|V|\,|[V]| = N$. Αφού ο V είναι κλειστός ως προς την πρόσθεση είναι εύκολο να ελέγξουμε ότι αν $\gamma \notin [V]$ τότε $\widehat{V}(\gamma) = 0$, και αν $\gamma \in [V]$ τότε $\widehat{V}(\gamma) = |V|$, οπότε η ταυτότητα Parseval μας δίνει

$$|V|N = \sum_{\gamma} |\widehat{V}(\gamma)|^2 = \sum_{\gamma \in [V]} |\widehat{V}(\gamma)|^2 = |[V]|\,|V|^2,$$

το οποίο δείχνει τον ισχυρισμό. Στη συνέχεια το λήμμα προκύπτει εύκολα. □

Πόρισμα 3.6.2. *Αν το B είναι χώρος Bohr και $c \in \mathcal{U}_N \setminus \{0\}$ τότε το $c \cdot B$ είναι επίσης χώρος Bohr και*

$$\mathrm{rk}(c \cdot B) = \mathrm{rk}(B).$$

Αφού οι χώροι Bohr είναι κλειστοί ως προς την πρόσθεση, το Θεώρημα 3.5.5 παίρνει την ακόλουθη πολύ απλή μορφή σε αυτό το πλαίσιο.

Θεώρημα 3.6.3. *Έστω $B \subset \mathcal{U}_N$ ένας χώρος Bohr και έστω $A_1, A_2, A_3 \subset B$ με σχετικές πυκνότητες $\alpha_i = |A_i|/|B|$. Έστω $\alpha = \min(\alpha_1, \alpha_2, \alpha_3)$. Τότε είτε*

$$\langle A_1 * A_2, A_3 \rangle \gg \alpha_1 \alpha_2 \alpha_3 |B|^2$$

ή υπάρχει χώρος Bohr $B' \subset B$ με τάξη

$$\mathrm{rk}(B') \leqslant \mathrm{rk}(B) + O(\mathcal{L}(\alpha)\alpha^{-1})$$

για τον οποίο μπορούμε να βρούμε $x \in \mathcal{U}_N$ και $i \in \{2, 3\}$ τέτοια ώστε

$$|(A_i - x) \cap B'| \geqslant (1 + \Omega(1))\alpha_i |B'|.$$

Μπορούμε στη συνέχεια να επαναλάβουμε αυτό το θεώρημα αύξησης της πυκνότητας με τον συνηθισμένο τρόπο και να δώσουμε ένα κάτω φράγμα για την ποσότητα $\Upsilon_{\mathbf{c}}(A)$, από το οποίο έπεται εύκολα το Θεώρημα 3.1.4.

Θεώρημα 3.6.4. *Έστω $\mathbf{c} = (c_1, c_2, c_3) \in (\mathbb{F}_q[t] \setminus \{0\})^3$ τέτοιο ώστε $c_1 + c_2 + c_3 = 0$ και έστω N αρκετά μεγάλος φυσικός που εξαρτάται μόνο από το $\mathbf{c}$. Για κάθε $A \subset \mathcal{U}_N$ ισχύει*

$$\Upsilon_{\mathbf{c}}(A) \geqslant \exp_q(-O_{\mathbf{c}}(\mathcal{L}(\alpha)^2\alpha^{-1}))N^2.$$

Απόδειξη. Θέτουμε $\ell = \max_{1 \leqslant i \leqslant 3} \deg c_i$. Έστω K ο μέγιστος φυσικός για τον οποίο υπάρχει ακολουθία χώρων Bohr

$$\mathcal{U}_N = B_0 \supset B_1 \supset \cdots \supset B_K,$$

και έστω ακολουθία συνόλων $A_i \subset B_i$ με πυκνότητες $\alpha_i = |A_i|/|B_i|$ τέτοια ώστε, για $0 \leqslant i < K$, υπάρχουν Λ_{i+1} με πληθάριθμο $O(\mathcal{L}(\alpha)\alpha_i^{-1})$ και $a_i \in \mathcal{U}_N \setminus \{0\}$ τέτοια ώστε να υπάρχουν Γ_i με $B_i = B(\Gamma_i)$ και

$$\Gamma_{i+1} \subset (a_i \cdot \{1, \ldots, t^{3\ell}\} \cdot \Gamma_i) \cup \Lambda_{i+1} \tag{3.6.3}$$

και για κάποια απόλυτη σταθερά $c > 0$ να έχουμε

$$\alpha_{i+1} \geqslant (1 + c)\alpha_i,$$

και επιπλέον $\Upsilon_{\mathbf{c}}(A_{i+1}) \leqslant \Upsilon_{\mathbf{c}}(A_i)$. Ειδικότερα,

$$1 \geqslant \alpha_k \geqslant (1 + c)^K \alpha,$$

συνεπώς $K \ll \mathcal{L}(\alpha)$. Από την (3.6.3) και με επαγωγή βλέπουμε ότι για $1 \leqslant J \leqslant K$, αν $\Lambda_0 = \{0\}$, υπάρχουν $a'_j \in \mathcal{U}_N \setminus \{0\}$ για $0 \leqslant j < J$ τέτοια ώστε

$$\Gamma_J \subset \Lambda_J \cup \bigcup_{j=0}^{J-1} a'_j \cdot \{1, \ldots, t^{3\ell(J-j)}\} \cdot \Lambda_j,$$

άρα ειδικότερα

$$\mathrm{rk}(B_K) \ll_\ell K \sum_{j=0}^{K} |\Lambda_j| \ll_\ell K\mathcal{L}(\alpha)\alpha^{-1} \sum_{i=0}^{K-1} (1+c)^{-i} \ll_\ell \mathcal{L}(\alpha)^2\alpha^{-1}. \tag{3.6.4}$$

Θα δείξουμε ότι

$$\Upsilon_{\mathbf{c}}(A_K) \gg \alpha^3 |B_K|^2 \tag{3.6.5}$$

και το θεώρημα έπεται από τις (3.6.2) και (3.6.4).

Θέτουμε $B' = B(\{1, \dots, t^{3\ell}\} \cdot \Gamma_K)$. Παρατηρούμε ότι $a \cdot B' \subset B_K$ για κάθε $a \in \mathbb{F}_q[t]$ με $\deg a \leqslant 3\ell$ και αν B'' είναι ένας χώρος Bohr της μορφής $a \cdot B'$ με $a \neq 0$ τότε

$$[B''] \subset a^{-1} \cdot \{1, \dots, t^{3\ell}\} \cdot \Gamma_K.$$

Θέτουμε $B'' = c_1 c_2 c_3 \cdot B'$ και $B^{(i)} = c_i^{-1} \cdot B''$ για $1 \leqslant i \leqslant 3$. Αφού $B^{(i)} \subset B_K$ για $1 \leqslant i \leqslant 3$,

$$\sum_{x \in B_K} (A_K * B^{(1)} + A_K * B^{(2)} + A_K * B^{(3)})(x) = 3|A_K|,$$

άρα για κάποιο $x \in B_K$ έχουμε

$$A_K * B^{(1)}(x) + A_K * B^{(2)}(x) + A_K * B^{(3)}(x) \geqslant 3\alpha_K.$$

Αν για κάποιο $1 \leqslant i \leqslant 3$ έχουμε $A_K * B^{(i)}(x) \geqslant \alpha_K(1+c)$ τότε έχουμε άτοπο από τη μεγιστικότητα του K θέτοντας $B_{K+1} = B^{(i)}$ και $A_{K+1} = A_K - x$. Αλλιώς, για κάθε $1 \leqslant i \leqslant 3$,

$$A_K * B^{(i)}(x) \geqslant (1-4c)\alpha_K.$$

Αν θέσουμε $A'_i = c_i \cdot ((A_K - x) \cap B'')$ τότε ικανοποιούνται οι υποθέσεις που απαιτούνται για να εφαρμόσουμε το Θεώρημα 3.6.3. Έπεται ότι είτε ισχύει η (3.6.5) ή μπορούμε να επιλέξουμε ως B_{K+1} το υπο-Bohr σύνολο του B_K που έχει έλεγχο του Λ και ως A_{K+1} μια μεταφορά κάποιου A'_i. Αφού

$$|\Lambda| = O(\alpha_K^{-1}\mathcal{L}(\alpha))$$

και

$$\alpha_{K+1} \geqslant (1 + \Omega(1))(1-4c)\alpha_K \geqslant (1+c)\alpha_K$$

αν επιλέξουμε το c αρκετά μικρό, αυτό έρχεται σε αντίφαση με τη μεγιστικότητα του K και έτσι ολοκληρώνεται η απόδειξη. □

3.7 Ακέραιοι

Σε αυτή την ενότητα αποδεικνύουμε το Θεώρημα 3.1.3 εφαρμόζοντας τις μεθόδους της προηγούμενης ενότητας στην περίπτωση $G = \mathbb{Z}_N$, όπου N είναι κάποιος μεγάλος πρώτος. Όπως και στην περίπτωση $G = \mathcal{U}_N$ σταθεροποιούμε κάποιους συντελεστές $c_1, c_2, c_3 \in \mathbb{Z} \setminus \{0\}$, πρώτους προς τον N, τέτοιους ώστε $c_1 + c_2 + c_3 = 0$ και για κάθε $A \subset \mathbb{Z}_N$ ορίζουμε την ποσότητα $\Upsilon_{\mathbf{c}}(A)$ όπως στην (3.6.1). Για κάθε $\Gamma \subset \widehat{\mathbb{Z}_N}$ και $\rho : \Gamma \to [0,2]$ ορίζουμε το σύνολο Bohr

$$B_\rho(\Gamma) = \{n \in \mathbb{Z}_N : |\gamma(n) - 1| < \rho(\gamma)\}.$$

Το Γ ονομάζεται σύνολο συχνοτήτων του B και η ρ ονομάζεται πλάτος. Ορίζουμε επίσης την τάξη του B να είναι ο πληθάριθμος του Γ. Με τον όρο σύνολο Bohr αναφερόμαστε στην τριάδα $(\Gamma, \rho, B_\rho(\Gamma))$ διότι το σύνολο $B_\rho(\Gamma)$ δεν προσδιορίζει μονοσήμαντα το σύνολο συχνοτήτων ή το πλάτος. Αν $\rho : \Gamma \to [0,2]$ και $\rho' : \Gamma' \to [0,2]$ τότε ορίζουμε την $\rho \wedge \rho' : \Gamma \cup \Gamma' \to [0,2]$ θέτοντας

$$\begin{aligned}(\rho \wedge \rho')(\gamma) &= \rho(\gamma) \quad \text{αν} \quad \gamma \in \Gamma \setminus \Gamma' \\ &= \rho'(\gamma) \quad \text{αν} \quad \gamma \in \Gamma' \setminus \Gamma \\ &= \min(\rho(\gamma), \rho(\gamma)) \quad \text{αν} \quad \gamma \in \Gamma \cap \Gamma'.\end{aligned}$$

Στην περίπτωση που μελετάμε εδώ, δεν έχουμε πλέον το πλεονέκτημα τα σύνολα Bohr να είναι κλειστά ως προς την πρόσθεση, όμως ο Bourgain παρατήρησε ότι κάποια σύνολα Bohr ικανοποιούν μια ασθενή εκδοχή αυτής της ιδιότητας η οποία είναι κατάλληλη για τις εφαρμογές που μας ενδιαφέρουν. Λέμε ότι ένα σύνολο Bohr τάξης d είναι κανονικό αν για κάθε $|\kappa| \leqslant 2^{-6}d^{-1}$ ισχύει

$$\big| |B_{\rho(1+\kappa)}(\Gamma)| - |B_\rho(\Gamma)| \big| \leqslant 2^6 d|\kappa|\,|B_\rho(\Gamma)|.$$

Αν $B = B_\rho(\Gamma)$ τότε γράφουμε $B(\lambda)$ για το σύνολο Bohr $B_{\lambda\rho}(\Gamma)$. Στο βιβλίο των Tao και Vu δίνονται οι αποδείξεις των ακόλουθων βασικών λημμάτων για τα σύνολα Bohr.

Λήμμα 3.7.1. *Για κάθε σύνολο Bohr B υπάρχει $\lambda \in [1/2, 1]$ τέτοιο ώστε το $B(\lambda)$ να είναι κανονικό.*

Λήμμα 3.7.2. *Αν $\rho' : \Gamma' \to [0,2]$ τότε*

$$|B_{\rho\wedge\rho'}(\Gamma \cup \Gamma')| \geqslant \prod_{\gamma\in\Gamma'} (\rho'(\gamma)/4)|B_\rho(\Gamma)|.$$

Επιπλέον, αν B είναι ένα σύνολο Bohr τάξης d τότε $|B(\lambda)| \geqslant \lambda^{O(d)}|B|$.

Το επόμενο λήμμα προκύπτει εύκολα από την παρατήρηση ότι αν $c \in \mathbb{Z}_N \setminus \{0\}$ τότε $c \cdot B_\rho(\Gamma) = B_\rho(c \cdot \Gamma)$.

Λήμμα 3.7.3. *Για κάθε σύνολο Bohr B και $c \in \mathbb{Z}_N^*$ το σύνολο $c \cdot B$ είναι επίσης σύνολο Bohr τάξης $\mathrm{rk}(B)$, και επιπλέον για κάθε $\lambda > 0$ ισχύει*

$$c \cdot (B(\lambda)) = (c \cdot B)(\lambda).$$

Η κανονικότητα μας επιτρέπει να πετύχουμε τον προσθετικό έλεγχο που χρειαζόμαστε, και το Θεώρημα 3.5.5 παίρνει την ακόλουθη μορφή.

Θεώρημα 3.7.4. *Υπάρχει απόλυτη σταθερά $c > 0$ τέτοια ώστε να ισχύουν τα ακόλουθα. Έστω $B \subset \mathbb{Z}_N$ ένα κανονικό σύνολο Bohr τάξης $d \leqslant \exp(c\mathcal{L}(\alpha)^2)$. Έστω $A_1, A_2 \subset B$ και $A_3 \subset B(\delta)$ με σχετικές πυκνότητες α_i. Θέτουμε $\alpha = \min(c, \alpha_1, \alpha_2, \alpha_3)$ και υποθέτουμε ότι το $B(\delta)$ είναι επίσης κανονικό και $cd^{-1}\alpha/4 \leqslant \delta \leqslant cd^{-1}\alpha$. Τότε είτε*

$$\langle A_1 * A_2, A_3 \rangle \gg \alpha_1\alpha_2\alpha_3 |B|\,|B(\delta)| \tag{3.7.1}$$

ή υπάρχει κανονικό σύνολο Bohr B' τάξης

$$\mathrm{rk}(B') \leqslant d + O(\mathcal{L}(\alpha)\alpha^{-1})$$

με πληθάριθμο

$$|B'| \geqslant \exp(-O(\mathcal{L}(\alpha)^2(d + \mathcal{L}(\alpha)\alpha^{-1})))|B| \tag{3.7.2}$$

τέτοιο ώστε να υπάρχουν $x \in \mathbb{Z}_N$ και $i \in \{1, 2\}$ με

$$|(A_i - x) \cap B'| \geqslant (1 + c)\alpha_i |B'|.$$

Απόδειξη. Αρχικά παρατηρούμε ότι αφού το B είναι κανονικό έχουμε

$$|(B(\delta) + B) \setminus B| \ll d\delta|B| \leqslant 2^{-2}\alpha|B|, \tag{3.7.3}$$

αρκεί το δ να είναι αρκετά μικρό. Τώρα ικανοποιούνται οι υποθέσεις του Θεωρήματος 3.5.5 άρα είτε ισχύει η (3.7.1) ή υπάρχει κάποιο πεπερασμένο σύνολο $\Lambda \subset \widehat{G}$ με πληθάριθμο $\ell = O(\mathcal{L}(\alpha)\alpha^{-1})$ τέτοιο ώστε αν ένα συμμετρικό σύνολο B' έχει $(4\ell)^{-1}$-έλεγχο του Λ, και ισχύουν οι

$$|(2B' + B) \setminus B| \leqslant 2^{-19}\alpha|B| \tag{3.7.4}$$

και

$$|(B' + B(\delta)) \setminus B(\delta)| \leqslant 2^{-4}\exp(-2^5\mathcal{L}(\alpha)^2)|B(\delta)| \tag{3.7.5}$$

τότε υπάρχουν $x \in \mathbb{Z}_N$ και $i \in \{1,2\}$ τέτοια ώστε

$$|(A_i - x) \cap B'| \geqslant (1 + 2^{-18})\alpha_i |B'|.$$

Έστω $\rho' : \Lambda \to [0,2]$ η συνάρτηση με $\rho'(\lambda) = 1/4\ell$ για κάθε $\lambda \in \Lambda$. Αν $B = B_\rho(\Gamma)$ τότε θέτουμε $B^* = B_{\delta\rho \wedge \rho'}(\Gamma \cup \Lambda)$, και $B' = B^*(\delta')$ για κάποιο δ' που θα επιλεγεί αργότερα, αλλά έτσι ώστε το B' να είναι κανονικό. Προφανώς, το B' είναι ένα κανονικό σύνολο Bohr τάξης $d + O(\mathcal{L}(\alpha)\alpha^{-1})$ που έχει $(4\ell)^{-1}$-έλεγχο του Λ από την επιλογή της ρ'. Αν $\delta' \leqslant 1/2$ τότε έχουμε ότι $2B' \subset B(\delta)$, άρα βλέπουμε ότι ικανοποιείται η (3.7.4), με ένα επιχείρημα όπως αυτό για την (3.7.3). Επιπλέον, αφού το $B(\delta)$ είναι κανονικό και $B' \subset B(\delta\delta')$ έπεται ότι

$$|(B' + B(\delta)) \setminus B(\delta)| \ll d\delta' |B(\delta)|,$$

άρα η (3.7.5) ικανοποιείται για κάποιο $\delta' \gg \exp(-O(\mathcal{L}(\alpha^2)))d^{-1}$. Τέλος, από το Λήμμα 3.7.2 έχουμε

$$|B'| \geqslant (\delta')^{O(\ell+d)}|B^*| \geqslant \ell^{-O(\ell)}\delta^d(\delta')^{O(\ell+d)}|B|,$$

και η (3.7.2) έπεται από τα φράγματα για τα δ, δ' και ℓ. Έτσι ολοκληρώνεται η απόδειξη. □

Μπορούμε τώρα να επαναλάβουμε το λήμμα της αύξησης πυκνότητας με τον συνήθη τρόπο για να δώσουμε ένα κάτω φράγμα για την $\Upsilon_{\mathbf{c}}(A)$.

Θεώρημα 3.7.5. *Έστω $\mathbf{c} \in (\mathbb{Z} \setminus \{0\})^3$ τέτοιο ώστε $c_1 + c_2 + c_3 = 0$. Για κάθε αρκετά μεγάλο πρώτο N, ο οποίος εξαρτάται μόνο από το $\mathbf{c}$, και κάθε $A \subset \mathbb{Z}_N$, έχουμε*

$$\Upsilon_{\mathbf{c}}(A) \geqslant \exp(-O_{\mathbf{c}}(\mathcal{L}(\alpha)^4\alpha^{-1}))N^2.$$

Για να πάρουμε το Θεώρημα 3.1.3 εμφυτεύουμε το $\{1,\dots,N\}$ σε κατάλληλο υποδιάστημα I του $\mathbb{Z}_{N'}$ όπου $N' \ll_{\mathbf{c}} N$ είναι κάποιος πρώτος αρκετά μεγάλος ώστε αν $x_1, x_2, x_3 \in I$ είναι μια λύση της εξίσωσης $c_1x_1 + c_2x_2 + c_3x_3 = 0$ στο $\mathbb{Z}_{N'}$ να είναι επίσης λύση της στο $\{1,\dots,N\}$.

Απόδειξη. Έστω K ο μέγιστος φυσικός για τον οποίο υπάρχει ακολουθία κανονικών συνόλων Bohr

$$\mathbb{Z}_N = B_0 \supset B_1 \supset \cdots \supset B_K,$$

καθένα με σύνολο συχνοτήτων Γ_i, τάξη d_i, πλάτος ρ_i, και μια ακολουθία συνόλων $A_i \subset B_i$ με πυκνότητα $\alpha_i = |A_i|/|B_i|$ τέτοια ώστε, για $0 \leqslant i < K$ να έχουμε

$$d_{i+1} \leqslant d_i + O(\mathcal{L}(\alpha)\alpha_i^{-1}) \leqslant \exp(O(\mathcal{L}(\alpha)^2)),$$

$$|B_{i+1}| \geqslant \exp(-O(\mathcal{L}(\alpha)^2(d_i + \mathcal{L}(\alpha)\alpha_i^{-1})))|B_i|, \tag{3.7.6}$$

$$\alpha_{i+1} \geqslant (1+c)\alpha_i,$$

και επιπλέον $\Upsilon_{\mathbf{c}}(A_{i+1}) \leqslant \Upsilon_{\mathbf{c}}(A_i)$. Ειδικότερα, αυτό ισχύει αν το A_{i+1} είναι υποσύνολο ενός πολλαπλασίου μιας μεταφοράς του A_i. Παρατηρούμε ότι

$$1 \geqslant \alpha_K \geqslant (1+c)^K \alpha,$$

άρα $K \ll \mathcal{L}(\alpha)$. Επιπλέον, για $0 \leqslant j \leqslant K$ έχουμε την εκτίμηση $d_j \ll \mathcal{L}(\alpha)\alpha^{-1}$, άρα

$$|B_K| \geqslant \exp\left(-O_{\mathbf{c}}\left(\mathcal{L}(\alpha)^2 \sum_{i=0}^{K} d_i\right)\right) N \geqslant \exp(-O(\mathcal{L}(\alpha)^4\alpha^{-1}))N.$$

Θα δείξουμε ότι

$$\Upsilon_{\mathbf{c}}(A_K) \gg \exp(-O(d_K\mathcal{L}(\alpha)^2))|B_K|^2,$$

και από αυτό έπεται το θεώρημα.

Για συντομία θέτουμε $B' = B_K(\rho')$, $B'' = B'(\rho') = B_K(\rho'\rho'')$ και $B''' = B''(\rho''') = B_K(\rho'\rho''\rho''')$, όπου τα ρ', ρ'' και ρ''' θα επιλεγούν αργότερα, αλλά έτσι ώστε όλα τα σύνολα Bohr που θεωρούμε να είναι κανονικά. Θέτουμε

$$B^{(1)} = c_2c_3 \cdot B'', B^{(2)} = c_1c_3 \cdot B'', B^{(3)} = c_2c_3 \cdot B'''$$

οπότε ειδικότερα αν $\rho'' \ll 1/c_1c_2c_3$ έχουμε $B^{(i)} \subset B'$ για $1 \leqslant i \leqslant 3$, άρα από την κανονικότητα του B_K έχουμε

$$\left|\sum_{x\in B_K} A_K * B^{(i)}(x) - |A_K|\right| \leqslant |(B' + B_K) \setminus B_K| \ll d\rho'|B_K|.$$

Ειδικότερα, για κάθε $\varepsilon > 0$ μπορούμε να επιλέξουμε $\rho' \gg_\varepsilon d^{-1}\alpha_K$ ώστε

$$\sum_{x\in B_K} (A_K * B^{(1)} + A_K * B^{(2)} + A_K * B^{(3)})(x) \geqslant (3-\varepsilon)|A_K|,$$

άρα, για κάποιο $x \in B$,

$$A_K * B^{(1)}(x) + A_K * B^{(2)}(x) + A_K * B^{(3)}(x) \geqslant (3-\varepsilon)\alpha_K.$$

Αν $A_K * B^{(i)}(x) \geqslant \alpha(1+c)$ για κάποιον $1 \leqslant i \leqslant 3$ τότε έχουμε άτοπο λόγω της μεγιστικότητας του K, θέτοντας $B_{K+1} = B^{(i)}$ και $A_{K+1} = (A_K - x) \cap B_{K+1}$. Ειδικότερα, παρατηρούμε ότι το $B^{(i)}$ έχει επίσης τάξη d_K και

$$|B^{(i)}| \geqslant |B''| \geqslant \exp(-O(d_K\mathcal{L}(\rho'\rho''\rho''')))|B_K|,$$

και θα δούμε ότι οι επιλογές μας για τις παραμέτρους ρ δίνουν το κάτω φράγμα (3.7.6). Αλλιώς, για $1 \leqslant i \leqslant 3$, αν επιλέξουμε το ε αρκετά μικρό, να εξαρτάται από το $\mathbf{c}$, τότε για $1 \leqslant i \leqslant 3$

$$A_K * B^{(i)}(x) \geqslant (1-c)\alpha_K.$$

Θέτουμε $A_i = c_i \cdot (A' - x) \cap c_i \cdot B^{(i)}$, και παρατηρούμε ότι

$$c_3 \cdot B^{(3)} = c_1 c_2 c_3 \cdot B''' \subset (c_1 c_2 c_3 \cdot B'')(\rho'''),$$

άρα υπάρχει $\rho''' \gg d_K^{-1}\alpha_K$ τέτοιος ώστε να μπορούμε να εφαρμόσουμε το Θεώρημα 3.7.4. Ειδικότερα, είτε

$$\Upsilon_{\mathbf{c}}(A_K) \gg \alpha_K^3 |B''|\,|B'''| \gg \exp(-O(d_K \mathcal{L}(\alpha)^2))|B_K|^2$$

ή υπάρχει κάποιο κανονικό σύνολο Bohr $B^{\#}$ με τάξη

$$d^{\#} \leqslant d + O(\mathcal{L}(\alpha)\alpha_K^{-1})$$

και πληθάριθμο

$$|B^{\#}| \geqslant \exp(-O(\mathcal{L}(\alpha)^2(d+\mathcal{L}(\alpha)\alpha_K^{-1})))|B''| \geqslant \exp(-O(\mathcal{L}(\alpha)^2(d+\mathcal{L}(\alpha)\alpha_K^{-1})))|B_K|,$$

και $i \in \{1, 2\}$ ώστε

$$|(A_i - x) \cap B^{\#}| \geqslant (1+\Omega(1))(1-c)\alpha_K|B^{\#}| \geqslant (1+c)\alpha_K|B^{\#}|,$$

αν επιλέξουμε το c αρκετά μικρό, το οποίο είναι άτοπο από τη μεγιστικότητα του K. Αυτό ολοκληρώνει την απόδειξη. $\square$

ΚΕΦΑΛΑΙΟ 4

Η πιθανοθεωρητική μέθοδος των Croot και Sisask

Έστω G μια ομάδα και $f, g : G \to \mathbb{C}$. Η συνέλιξη των f και g είναι η συνάρτηση $f * g$ που ορίζεται από την

$$f * g(x) := \sum_{y \in G} f(y)g(y^{-1}x),$$

αν βέβαια το άθροισμα αυτό είναι καλά ορισμένο για κάθε $x \in G$. Αρκετά από τα κεντρικά αντικείμενα μελέτης της προσθετικής συνδυαστικής εκφράζονται συναρτήσει συνελίξεων: για παράδειγμα, το σύνολο γινομένων $A \cdot B = \{ab : a \in A, b \in B\}$ των A και B είναι ακριβώς ο φορέας της συνάρτησης $\mathbf{1}_A * \mathbf{1}_B$, όπου $\mathbf{1}_X$ είναι η δείκτρια συνάρτηση ενός συνόλου X, και το πλήθος των αριθμητικών προόδων με τρεις όρους σε ένα προσθετικό σύνολο A, δηλαδή το πλήθος των τριάδων $(a_1, a_2, a_3) \in A \times A \times A$ που ικανοποιούν την $a_1 + a_3 = 2a_2$, είναι ίσο με $\mathbf{1}_A * \mathbf{1}_{2 \cdot A} * \mathbf{1}_A(0)$.

Οι Croot και Sisask παρουσιάζουν μια νέα τεχνική, η οποία δίνει αποτελέσματα για συνελίξεις, αντίστοιχα με αποτελέσματα που αποδεικνύονται με μεθόδους της Ανάλυσης Fourier, τα οποία όμως ισχύουν σε τυχούσες ομάδες και έχουν εφαρμογές στην προσθετική συνδυαστική.

4.1 Στοιχεία προσθετικής συνδυαστικής

Σε αυτή την ενότητα περιγράφουμε κάποια βασικά αποτελέσματα της προσθετικής συνδυαστικής για συνελίξεις και γινόμενα συνόλων. Ξεκινάμε εισάγοντας κάποιο συμβολισμό. Με G συμβολίζουμε μια ομάδα, η οποία ενδέχεται να είναι άπειρη. Αν A και B είναι δύο υποσύνολα της G, γράφουμε $A \cdot B = \{ab : a \in A, b \in B\}$ για το σύνολο γινομένων των A και B, και A^{-1} για το σύνολο των αντιστρόφων των στοιχείων του A. Για δοθέν $t \in G$ ορίζουμε $tA := \{ta : a \in A\}$ να είναι η αριστερή μεταφορά του A κατά t, και ανάλογα ορίζουμε την δεξιά μεταφορά At. Αν k είναι ένας θετικός ακέραιος, γράφουμε $A^k := A \cdot A \cdots A$ για την k-οστή δύναμη του A και A^{-k} για την k-οστή δύναμη του A^{-1}. Στο πλαίσιο των αβελιανών ομάδων συμβολίζουμε την πράξη της ομάδας με $+$ και δίνουμε τους αντίστοιχους ορισμούς για τα $A+B$, $A-B$, $t+A$, kA, κλπ.

Η πολλαπλασιαστική ενέργεια μεταξύ δύο συνόλων ορίζεται να είναι η ποσότητα

$$E(A,B) := \sum_{x \in G} \mathbf{1}_A * \mathbf{1}_B(x)^2.$$

Όταν μιλάμε για αβελιανές ομάδες ονομάζουμε αυτή την ποσότητα προσθετική ενέργεια. Για κάθε συνάρτηση $f : G \to \mathbb{C}$ και κάθε $p \geqslant 1$ θέτουμε

$$\|f\|_p^p = \sum_{x \in G} |f(x)|^p$$

αν το τελευταίο άθροισμα είναι πεπερασμένο. Με αυτό τον ορισμό έχουμε

$$E(A,B) = \|\mathbf{1}_A * \mathbf{1}_B\|_2^2.$$

Τέλος, για μια πεπερασμένη ομάδα G, η πυκνότητα ενός συνόλου $A \subseteq G$ είναι ο λόγος $|A|/|G|$.

Υπενθυμίζουμε ότι στο πλαίσιο των μη αβελιανών ομάδων η συνέλιξη παύει να είναι μεταθετική, είναι όμως διγραμμική και προσεταιριστική. Η σύνδεση της συνέλιξης με τα γινόμενα συνόλων προκύπτει από την παρατήρηση ότι ο φορέας της συνέλιξης $\mathbf{1}_{A_1} * \cdots * \mathbf{1}_{A_k}$ των δεικτριών συναρτήσεων των συνόλων $A_1, \ldots, A_k$ είναι το γινόμενο συνόλων $A_1 \cdots A_k$. Πιο συγκεκριμένα,

$$\mathbf{1}_{A_1} * \cdots * \mathbf{1}_{A_k}(x) = |\{(a_1, \ldots, a_k) \in A_1 \times \cdots \times A_k : a_1 \cdots a_k = x\}|. \tag{4.1.1}$$

Με άλλα λόγια, η συνέλιξη μετράει το πλήθος των αναπαραστάσεων ενός στοιχείου του $A_1 \times \cdots \times A_k$ ως γινομένου στοιχείων αυτών των k συνόλων. Στην περίπτωση $k = 2$ μπορούμε επίσης να γράφουμε

$$\mathbf{1}_A * \mathbf{1}_B(x) = |A \cap xB^{-1}| = |B \cap A^{-1}x|.$$

Αυτή η εναλλαγή μεταξύ αριστερών και δεξιών μεταφορών, όταν μιλάμε για γενικές συναρτήσεις, εκφράζεται από την

$$\widetilde{f * g} = \tilde{g} * \tilde{f}, \tag{4.1.2}$$

όπου $\tilde{f}(x) := f(x^{-1})$. Σημειώνουμε ότι $\widetilde{\mathbf{1}_X} = \mathbf{1}_{X^{-1}}$. Προσθέτοντας πάνω από όλα τα $x \in G$ παίρνουμε

$$\sum_{x\in G} \mathbf{1}_{A_1} * \cdots * \mathbf{1}_{A_k}(x) = |A_1| \cdots |A_k|. \tag{4.1.3}$$

Αν A και B είναι δύο πεπερασμένα υποσύνολα μιας ομάδας G, ισχύουν πάντα οι ανισότητες

$$\max\{|A|, |B|\} \leqslant |A \cdot B| \leqslant |A|\,|B|.$$

Ισότητα μπορεί σε ορισμένες περιπτώσεις να ισχύει, τόσο στη μία όσο και στην άλλη ανισότητα. Ισχύει, φυσικά, επίσης η ανισότητα $|A \cdot B| \leqslant |G|$. Μεγάλη σημασία σε αυτό το κεφάλαιο έχουν οι περιπτώσεις όπου το σύνολο γινομένων $A \cdot B$ είναι μικρό. Γενικά, λέμε ότι το $|A \cdot B|$ είναι μικρό αν φράσσεται από $K|A|$ ή $K|B|$ για κάποια σταθερά K, δηλαδή είναι περίπου ίσο με την ελάχιστη τιμή που θα μπορούσε να πάρει. Σκεφτόμαστε ότι μια ανισότητα της μορφής $|A \cdot B| \leqslant K|B|$ δείχνει ότι τα A και B έχουν κοινή δομή, ειδικά στην περίπτωση που τα A και B έχουν περίπου τον ίδιο πληθάριθμο. Ειδικότερα, αυτό έχει σαν συνέπεια ότι τα A και B πρέπει κι αυτά τα ίδια να έχουν κάποια δομή.

Λήμμα 4.1.1 (τριγωνική ανισότητα του Ruzsa)**.** *Έστω A, B, C πεπερασμένα μη κενά υποσύνολα μιας ομάδας G. Τότε*

$$|A \cdot C^{-1}| \leqslant \frac{|A \cdot B^{-1}|\,|B \cdot C^{-1}|}{|B|}.$$

Τα θεωρήματα σχεδόν περιοδικότητας που θα δείξουμε είναι ισχυρά όταν ένα από τα σύνολα A και B είναι δομημένο με την έννοια ότι έχει μικρό τετράγωνο, δηλαδή είτε $|A^2| \leqslant K|A|$ είτε $|B^2| \leqslant K|B|$, ή μικρό σύνολο διαφορών, δηλαδή είτε $|A \cdot A^{-1}| \leqslant K|A|$ είτε $|B \cdot B^{-1}| \leqslant K|B|$ για κάποια μικρή σταθερά K. Στο πλαίσιο των αβελιανών ομάδων, το επόμενο θεώρημα είναι πολύ χρήσιμο όταν θέλουμε να φράξουμε τον πληθάριθμο συνόλων αθροισμάτων.

Θεώρημα 4.1.2 (ανισότητα Plünnecke-Ruzsa)**.** *Έστω A και B πεπερασμένα υποσύνολα μιας αβελιανής ομάδας, και έστω ότι $|A + B| \leqslant K|A|$. Τότε*

$$|nB - mB| \leqslant K^{m+n}|A|$$

για κάθε $m, n \geqslant 1$.

Μπορούμε όμως να αντικαταστήσουμε την παραπάνω έννοια δομής με μία πολύ ασθενέστερη: αυτήν του να είναι κάποιο σύνολο πυκνό σε ένα δομημένο σύνολο. Υπάρχουν κι άλλοι τρόποι με τους οποίους μπορούμε να εξασθενίσουμε την έννοια της δομής που χρησιμοποιούμε. Υπενθυμίζουμε τον ορισμό της πολλαπλασιαστικής ενέργειας μεταξύ δύο συνόλων:

$$E(A,B)=\sum_{x\in G}\mathbf{1}_A*\mathbf{1}_B(x)^2.$$

Αν το σύνολο γινομένων $A\cdot B$ έχει μικρό πληθάριθμο συγκρινόμενο με αυτόν του A ή του B, με την έννοια ότι είναι το πολύ ίσος με $K|A|$ ή $K|B|$, τότε η ενέργεια $E(A,B)$ είναι μεγάλη. Εχουμε

$$E(A,B)\geqslant\frac{1}{|A\cdot B|}\left(\sum_{x\in G}\mathbf{1}_A*\mathbf{1}_B(x)\right)^2=\frac{|A|^2|B|^2}{|A\cdot B|}, \tag{4.1.4}$$

όπου η τελευταία ανισότητα προκύπτει από την ανισότητα Cauchy-Schwarz. Από την άλλη πλευρά, η συνθήκη

$$E(A,A)\geqslant|A|^3/K$$

δεν συνεπάγεται απαραίτητα ότι ο πληθάριθμος $|A^2|$ είναι μικρός, ακόμα και στο πλαίσιο των αβελιανών ομάδων. Ισχύει όμως ένα μερικό αντίστροφο, το θεώρημα Balog-Szemerédi-Gowers, το οποίο μπορεί να φανεί χρήσιμο σε κάποιες εφαρμογές, στις οποίες τα σύνολα που μελετάμε έχουν μεγάλη πολλαπλασιαστική ενέργεια αντί για μικρό τετράγωνο.

Πολλά από τα αποτελέσματα που αναφέραμε σε αυτή την ενότητα έχουν ανάλογα όπου θεωρούμε γενικές συναρτήσεις αντί για δείκτριες συναρτήσεις. Η διαφορά ανάμεσα σε δείκτριες συναρτήσεις και πιο γενικές συναρτήσεις δεν είναι πολύ σημαντική στην πράξη.

4.2 Σχεδόν περιοδικότητα

Στόχος μας είναι να παρουσιάσουμε μια πιθανοθεωρητική τεχνική των Croot και Sisask με την οποία μπορούμε να βρούμε «σχεδόν-περιόδους» συνελίξεων υποσυνόλων μιας ομάδας. Έτσι παίρνουμε αποτελέσματα παρόμοια με τα θεωρήματα τύπου Bogolyubov που προκύπτουν με μεθόδους ανάλυσης Fourier στις αβελιανές ομάδες, χωρίς να χρειαστούμε την ύπαρξη μετασχηματισμού Fourier με καλές ιδιότητες. Το πρώτο μας αποτέλεσμα είναι το ακόλουθο θεώρημα σχεδόν περιοδικότητας.

Πρόταση 4.2.1 (L^2-σχεδόν περιοδικότητα, τοπική μορφή)**.** *Έστω G μια ομάδα, A,B πεπερασμένα υποσύνολα της G και $\varepsilon\in(0,1)$ μια παράμετρος. Υποθέτουμε ότι για κάποιο $S\subseteq G$ ισχύει ότι $|B\cdot S|\leqslant K|B|$. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T|\geqslant\frac{|S|}{(2K)^{9/\varepsilon^2}}$$

τέτοιο ώστε, για κάθε $t\in TT^{-1}$,

$$\|\mathbf{1}_A*\mathbf{1}_B(xt)-\mathbf{1}_A*\mathbf{1}_B(x)\|_2^2\leqslant\varepsilon^2|A|\,|B|^2.$$

Η συνθήκη ότι πρέπει να υπάρχει κάποιο σύνολο S τέτοιο ώστε $|B \cdot S| \leqslant K|B|$ δικαιολογεί τον όρο «τοπική». Δεν χρειάζεται να έχουμε το B πυκνό στην G για να μπορούμε να εφαρμόσουμε αποτελεσματικά αυτή την πρόταση. Το μόνο που χρειαζόμαστε είναι το B να αλληλεπιδρά καλά με κάποιο μεγάλο σύνολο S, μια συνθήκη που θα συζητήσουμε πιο αναλυτικά παρακάτω. Ακόμα κι αν γνωρίζουμε λίγα πράγματα για τη δομή του B μπορούμε να πάρουμε χρήσιμες πληροφορίες από την πρόταση αν το B είναι πυκνό σε κάποιο δομημένο σύνολο. Για παράδειγμα, αν $G = \mathbb{Z}$ και $B \subseteq [N] := \{1..., N\}$ με $|B| \geqslant \beta N$ τότε μπορούμε βα πάρουμε $S = [N]$ και $K = 2/\beta$. Όμοια, αν η G είναι πεπερασμένη τότε μπορούμε πάντα να πάρουμε $S = G$, ανεξάρτητα από το B, και έχουμε άμεσα το ακόλουθο πόρισμα.

Πόρισμα 4.2.2 (L^2-σχεδόν περιοδικότητα, ολική μορφή). *Έστω G μια πεπερασμένη ομάδα, A, B υποσύνολα της G και $\varepsilon \in (0,1)$ μια παράμετρος. Υποθέτουμε ότι το B έχει πυκνότητα β. Τότε υπάρχει υποσύνολο T της G μεγέθους*

$$|T| \geqslant (\beta/2)^{9/\varepsilon^2}|G|$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \varepsilon^2 |A|\,|B|^2.$$

Τα προηγούμενα αποτελέσματα μας λένε ότι οι συνελίξεις είναι κατά κάποιον τρόπο συνεχείς. Μπορούμε να βρούμε μεγάλο πλήθος μεταφορών t ώστε η συνάρτηση $\mathbf{1}_A * \mathbf{1}_B$ να μην αλλάζει πολύ – με την L^2 έννοια – όταν την μεταφέρουμε κατά t. Έχοντας στη διάθεσή μας L^2-σχεδόν περιόδους έχουμε καλό έλεγχο για πολλές εφαρμογές, ειδικότερα σε καταστάσεις στις οποίες εμφανίζονται συνελίξεις βαθμού μεγαλύτερου από 2. Μια ενδιαφέρουσα περίπτωση είναι όταν μελετάμε το πλήθος των αριθμητικών προόδων μήκους 3 σε ένα σύνολο ή όταν μελετάμε ένα σύνολο τριπλών γινομένων $A \cdot B \cdot C$. Όμως, για κάποιες εφαρμογές στις οποίες μας ενδιαφέρει η συνήθης απλή συνέλιξη είναι πιο χρήσιμο να έχουμε L^p-σχεδόν περιόδους για μεγαλύτερες τιμές του p. Σε αυτή την κατεύθυνση έχουμε το εξής αποτέλεσμα.

Πρόταση 4.2.3 (L^p-σχεδόν περιοδικότητα, τοπική μορφή). *Έστω G μια ομάδα, A, B πεπερασμένα υποσύνολα της G και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι για κάποιο $S \subseteq G$ ισχύει ότι $|B \cdot S| \leqslant K|B|$. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T| \geqslant \frac{|S|}{(2K)^{50m/\varepsilon}}$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \max\{\varepsilon^m |AB|\,|B|^m, \|\mathbf{1}_A * \mathbf{1}_B\|_m^m\}\varepsilon^m |B|^m.$$

Όπως και προηγουμένως, παίρνουμε το ακόλουθο «ολικό» πόρισμα.

Πόρισμα 4.2.4 (L^p-σχεδόν περιοδικότητα, ολική μορφή)**.** *Έστω G μια πεπερασμένη ομάδα, A, B υποσύνολα της G και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι το B έχει πυκνότητα β. Τότε υπάρχει υποσύνολο T του S μεγέθους*

$$|T| \geqslant (\beta/2)^{50m/\varepsilon}|G|$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \max\{\varepsilon^m |AB|\,|B|^m, \|\mathbf{1}_A * \mathbf{1}_B\|_m^m\}\varepsilon^m |B|^m.$$

Θα αποδείξουμε κάποιες παραλλαγές αυτών των αποτελεσμάτων. Με μια μικρή αλλαγή στις υποθέσεις μπορούμε να βρούμε αριστερές μεταφορές αντί για δεξιές μεταφορές, κάτι που είναι πιο χρήσιμο στις εφαρμογές. Οι αποδείξεις αυτών των προτάσεων είναι πιθανοθεωρητικής φύσης, βασίζονται δηλαδή σε μια διαδικασία τυχαίας επιλογής με την οποία βρίσκουμε μικρά υποσύνολα ενός από τα σύνολα, που συμπεριφέρονται όμοια με το ίδιο το σύνολο, με μια έννοια που θα γίνει ακριβής. Αυτή η τυχαία διαδικασία είναι η ίδια, ανεξάρτητα από το αν η ομάδα είναι αβελιανή ή όχι, και αυτό είναι το νέο στοιχείο σε σύγκριση με τις μεθόδους της ανάλυσης Fourier τις οποίες χρησιμοποιούμε συνήθως όταν μελετάμε αβελιανές ομάδες.

Ζητάμε μεταφορές για τις οποίες η συνέλιξη $\mathbf{1}_A * \mathbf{1}_B$ είναι κατά προσέγγιση αναλλοίωτη ως προς κάποια νόρμα. Υπάρχουν δύο βασικές ιδέες πίσω από τις αποδείξεις αυτών των προτάσεων. Η πρώτη ιδέα είναι ότι αν επιλέξουμε ένα μικρό τυχαίο υποσύνολο $C \subseteq A$ τότε με μεγάλη πιθανότητα η συνέλιξη $\mathbf{1}_C * \mathbf{1}_B$ θα προσεγγίζει τη συνάρτηση $\frac{|C|}{|A|}\mathbf{1}_A * \mathbf{1}_B$. Αυτό σημαίνει ότι η προσέγγιση θα ισχύει για πολλά υποσύνολα C του A, τόσο πολλά που πρέπει να ισχύουν κάποιες σχέσεις ανάμεσα στα σύνολα: πολλά από αυτά πρέπει στην πραγματικότητα να είναι το ένα μεταφορά του άλλου. Αυτή είναι η δεύτερη ιδέα: οι μεταφορές που παίρνουμε αντιστοιχούν σε μεταφορές που αφήνουν την $\mathbf{1}_A * \mathbf{1}_B$ κατά προσέγγιση αναλλοίωτη ως προς κατάλληλη νόρμα.

Αποδεικνύουμε αρχικά την ακόλουθη ισοδύναμη μορφή της Πρότασης 4.2.1. Η ισοδυναμία προκύπτει άμεσα από την ταυτότητα ανάκλασης (4.1.2).

Πρόταση 4.2.5 (L^2-σχεδόν περιοδικότητα, αριστερές μεταφορές)**.** *Έστω G μια ομάδα, A, B πεπερασμένα υποσύνολα της G και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι για κάποιο $S \subseteq G$ ισχύει ότι $|S \cdot A| \leqslant K|A|$. Τότε υπάρχει υποσύνολο T του S^{-1} μεγέθους*

$$|T| \geqslant \frac{|S|}{(2K)^{9/\varepsilon^2}}$$

τέτοιο ώστε, για κάθε $t \in TT^{-1}$,

$$\|\mathbf{1}_A * \mathbf{1}_B(tx) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \varepsilon^2 |A|^2 |B|.$$

Απόδειξη. Θεωρούμε έναν φυσικό αριθμό k με $1 \leqslant k \leqslant |A|/2$ τον οποίο θα σταθεροποιήσουμε στη συνέχεια, και ένα τυχαίο υποσύνολο C του A με k στοιχεία, το οποίο επιλέγεται ομοιόμορφα πάνω από όλα αυτά τα υποσύνολα. Γράφουμε

$$\mu_C := \mathbf{1}_C \cdot \frac{|A|}{k}$$

για την κανονικοποιημένη δείκτρια συνάρτηση του C. Παρατηρούμε ότι

$$\mathbb{E}\mu_C * \mathbf{1}_B(x) = \mathbf{1}_A * \mathbf{1}_B(x)$$

για κάθε $x \in G$ και ότι η διασπορά

$$\mathrm{Var}(\mu_C * \mathbf{1}_B(x)) = \mathbb{E}|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)|^2$$

ικανοποιεί την

$$\mathrm{Var}(\mu_C * \mathbf{1}_B(x)) \leqslant \frac{|A|}{k}\mathbf{1}_A * \mathbf{1}_B(x).$$

Αθροίζοντας πάνω από όλα τα $x \in A \cdot B = \mathrm{supp}(\mathbf{1}_A * \mathbf{1}_B)$ παίρνουμε

$$\mathbb{E}\|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \frac{1}{k}|A|^2|B|. \tag{4.2.1}$$

Θα λέμε ότι ένα σύνολο $C \in \binom{G}{k}$ *προσεγγίζει* το A αν ισχύει η ανισότητα

$$\|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \frac{2}{k}|A|^2|B|.$$

Από την (4.2.1) και την ανισότητα Markov έχουμε ότι

$$\mathbb{P}_{C\in\binom{G}{k}}(\text{το } C \text{ προσεγγίζει το } A) \geqslant \frac{1}{2}. \tag{4.2.2}$$

Θεωρούμε τώρα σύνολα C με k στοιχεία που επιλέγονται τυχαία και ομοιόμορφα από το $Y := S \cdot A$ αντί για το A. Έστω $t \in S^{-1}$. Παρατηρούμε ότι

$$\mathbb{P}_{C\in\binom{Y}{k}}(\text{το } tC \text{ προσεγγίζει το } A) = \mathbb{P}_{C\in\binom{tY}{k}}(\text{το } C \text{ προσεγγίζει το } A),$$

και αφού $A \subseteq tY$ συμπεραίνουμε ότι αυτή η πιθανότητα είναι τουλάχιστον ίση με

$$\binom{|A|}{k}\binom{|S \cdot A|}{k}^{-1}\mathbb{P}_{C\in\binom{A}{k}}(\text{το } C \text{ προσεγγίζει το } A).$$

Από την (4.2.2) και την υπόθεση ότι $|S \cdot A| \leqslant K|A|$ έπεται ότι

$$\mathbb{P}_{C\in\binom{Y}{k}}(\text{το } tC \text{ προσεγγίζει το } A) \geqslant \frac{1}{(2K)^k}.$$

Αθροίζοντας αυτές τις ανισότητες πάνω από όλα τα $t \in S^{-1}$ παίρνουμε

$$\mathbb{E}_{C\in\binom{Y}{k}}|\{t \in S^{-1} : \text{το } tC \text{ προσεγγίζει το } A\}| \geqslant \frac{|S|}{(2K)^k}.$$

Ειδικότερα, υπάρχει κάποιο σύνολο C με την ιδιότητα ότι το

$$T := \{t \in S^{-1} : \text{το } tC \text{ προσεγγίζει το } A\}$$

έχει τουλάχιστον $|S|/(2K)^k$ στοιχεία. Γι' αυτό το σύνολο C έχουμε

$$\|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(tx)\|_2^2 \leqslant \frac{2}{k}|A|^2|B|$$

για κάθε $t \in T$, άρα

$$\|\mathbf{1}_A * \mathbf{1}_B(tx) - \mathbf{1}_A * \mathbf{1}_B(x)\|_2^2 \leqslant \frac{8}{k}|A|^2|B|$$

για κάθε $t \in TT^{-1}$, από την τριγωνική ανισότητα. Επιλέγοντας τώρα $k := \lfloor 8/\varepsilon^2 \rfloor$ έχουμε το ζητούμενο. Παρατηρήστε ότι το συμπέρασμα της πρότασης ισχύει τετριμμένα αν $k > |A|/2$. □

Για να αποδείξουμε την αντίστοιχη εκτίμηση για υψηλότερες L^p νόρμες χρησιμοποιούμε ροπές υψηλότερης τάξης αντί για τη διασπορά. Για το σκοπό αυτό χρειαζόμαστε περισσότερες πληροφορίες για τυχαίες μεταβλητές της μορφής $\mathbf{1}_C * \mathbf{1}_B(x)$. Δεδομένου ότι $\mathbf{1}_C * \mathbf{1}_B(x) = |C \cap xB^{-1}|$, βλέπουμε ότι αυτή η τυχαία μεταβλητή έχει υπεργεωμετρική κατανομή: λέμε ότι μια τυχαία μεταβλητή έχει υπεργεωμετρική κατανομή με παρραμέτρους N, M και k αν

$$\mathbb{P}(X = j) = \binom{M}{j}\binom{N-M}{k-j}\Big/\binom{N}{k}$$

για κάθε ακέραιο $j \geqslant 0$. Μπορούμε να σκεφτόμαστε ότι η X μετράει το πλήθος των σημειωμένων αντικειμένων που παίρνουμε όταν επιλέγουμε τυχαία και χωρίς αντικατάσταση k αντικείμενα από ένα σύνολο N αντικειμένων, από τα οποία M συνολικά είναι σημειωμένα. Θα χρειαστούμε την ακόλουθη εκτίμηση.

Λήμμα 4.2.6. *Έστω $m \geqslant 1$ και έστω ότι η X έχει την υπεργεωμετρική κατανομή με παραμέτρους N, M και k όπως παραπάνω. Τότε,*

$$\mathbb{E}\Big|X - \frac{kM}{N}\Big|^{2m} \leqslant 2\left(3m\frac{kM}{N} + m^2\right)^m.$$

Για την απόδειξη του Λήμματος 4.2.6 θα χρησιμοποιήσουμε την επόμενη πρόταση.

Πρόταση 4.2.7. *Έστω ότι η X έχει την υπεργεωμετρική κατανομή με παραμέτρους N, M και k και η Y έχει την διωνυμική κατανομή με παραμέτρους $n = k$ και $p = M/N$. Τότε, για κάθε συνεχή κυρτή συνάρτηση f έχουμε*

$$\mathbb{E}f(X) \leqslant \mathbb{E}f(Y).$$

Ειδικότερα, αν $m \geqslant 1/2$ τότε

$$\mathbb{E}\Big|X - \frac{kM}{N}\Big|^{2m} \leqslant \mathbb{E}|Y - np|^{2m}.$$

Έχοντας στη διάθεσή μας την Πρόταση 4.2.7 για την απόδειξη του Λήμματος 4.2.6 αρκεί να αποδείξουμε την ακόλουθη πρόταση.

Πρόταση 4.2.8. *Έστω $m \geqslant 1$ και έστω ότι η X έχει διωνυμική κατανομή με παραμέτρους n και p. Τότε*

$$\mathbb{E}|X - np|^{2m} \leqslant 2(3mnp + m^2)^m. \tag{4.2.3}$$

Με τη σειρά της, η απόδειξη της Πρότασης 4.2.8 βασίζεται στις ακόλουθες ανισότητες απόκλισης, τύπου Bennett, Bernstein, Chernoff και Hoeffding.

Πρόταση 4.2.9. *Έστω ότι η X έχει διωνυμική κατανομή με παραμέτρους n και p. Τότε*

$$\mathbb{P}(X \leqslant np - t) \leqslant \exp\Big(-\frac{t^2}{2np}\Big) \tag{4.2.4}$$

και

$$\mathbb{P}(X \geqslant np + t) \leqslant \exp\Big(-\frac{t^2}{2(np + t/3)}\Big) \tag{4.2.5}$$

για κάθε $t \geqslant 0$.

Οι εκτιμήσεις αυτές είναι κλασικές. Μπορεί κανείς να τις αποδείξει εφαρμόζοντας την ανισότητα Markov στην τυχαία μεταβλητή $e^{\lambda(X-np)}$, χρησιμοποιώντας το γεγονός ότι η ροπογεννήτρια $\mathbb{E}e^{\lambda(X-np)}$ ισούται με $e^{-\lambda pn}(pe^{\lambda} + 1 - p)^n$.

Απόδειξη της Πρότασης 4.2.8. Γράφουμε

$$\mathbb{E}|X - np|^{2m} = \int_0^\infty \mathbb{P}(|X - np|^{2m} > t)\, dt. \tag{4.2.6}$$

Αφού

$$\mathbb{P}(|X - np| > t) = \mathbb{P}(X < np - t) + \mathbb{P}(X > np + t),$$

μπορούμε να γράψουμε το δεξιό μέλος της (4.2.6) ως άθροισμα δύο ολοκληρωμάτων, κατά προφανή τρόπο, τα οποία συμβολίζουμε με I^- και I^+. Χρησιμοποιώντας τις εκτιμήσεις (4.2.4) και (4.2.5) παίρνουμε

$$I^- \leqslant \int_0^\infty \exp\Big(-\frac{t^{1/m}}{2np}\Big)\,dt = (2np)^m\Gamma(m+1)$$

και

$$I^+ \leqslant \int_0^\infty \exp\Big(-\frac{t^{1/m}}{2(np+t^{1/2m}/3)}\Big)\,dt.$$

Χωρίζουμε το διάστημα ολοκλήρωσης σε δύο μέρη ως εξής: Θέτουμε

$$\lambda := \frac{1}{3}+\frac{1}{3}\sqrt{1+6np/m},$$

οπότε $9(\lambda m)^2/2(np+\lambda m) = 3m$. Στη συνέχεια ορίζουμε I_1 το ολοκλήρωμα στο διάστημα $0 \leqslant t \leqslant (3\lambda m)^{2m}$ και I_2 το ολοκλήρωμα στο διάστημα που απομένει. Έτσι έχουμε

$$I_1 \leqslant \int_0^\infty \exp\Big(-\frac{t^{1/m}}{2(np+\lambda m)}\Big)\,dt = (2np+2\lambda m)^m\Gamma(m+1).$$

Για να φράξουμε το I_2 χρειάζεται λίγο περισσότερη προσοχή. Θέτουμε $w := \frac{9(\lambda m)^2}{2(mp+\lambda m)} = 3m$. Τότε,

$$I_2 \leqslant \int_{(3\lambda m)^{2m}}^\infty \exp\Big(-\frac{3t^{1/2m}}{2(1+np/\lambda m)}\Big)\,dt = 2m\Big(\frac{2(np+\lambda m)}{3\lambda m}\Big)^{2m}\int_w^\infty z^{2m-1}e^{-z}dz.$$

Με την αλλαγή μεταβλητής $u = z - w$, το τελευταίο ολοκλήρωμα γίνεται

$$w^{2m-1}e^{-w}\int_0^\infty \Big(1+\frac{u}{w}\Big)^{2m-1}e^{-u}du \leqslant w^{2m-1}e^{-w}\int_0^\infty e^{-u(1-2m/w)}du,$$

με την τελευταία ανισότητα να προκύπτει από την $1+x \leqslant e^x$ που ισχύει για κάθε x, και η τελευταία ποσότητα ισούται με $w^{2m}e^{-w}/m$. Έτσι έχουμε

$$I_2 \leqslant 2(3\lambda m)^{2m}e^{-3m}.$$

Συνδυάζοντας αυτές τις εκτιμήσεις για τα I^- και $I^+ = I_1 + I_2$ παίρνουμε

$$\mathbb{E}|X-np|^{2m} \leqslant (2np)^m\Gamma(m+1) + (2np+2\lambda m)^m\Gamma(m+1) + 2(9\lambda^2m^2/e^3)^m.$$

Χρησιμοποιώντας το φράγμα $\Gamma(m+1) \leqslant 2(3m/5)^m$ και τον ορισμό του λ καταλήγουμε στην (4.2.4). $\square$

Πρόταση 4.2.10 (L^p-σχεδόν περιοδικότητα, αριστερές μεταφορές)**.** *Έστω G μια ομάδα, A, B πεπερασμένα υποσύνολα της G, και $\varepsilon \in (0,1)$ και $m \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι S είναι ένα υποσύνολο της G με $|S \cdot A| \leqslant K|A|$. Τότε υπάρχει $T \subseteq S^{-1}$ με*

$$|T| \geqslant \frac{|S|}{(2K)^{50m/\varepsilon}}$$

τέτοιο ώστε

$$\|\mathbf{1}_A * \mathbf{1}_B(tx) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \max\{\varepsilon^m |AB|\,|A|^m, \|\mathbf{1}_A * \mathbf{1}_B\|_m^m\}\varepsilon^m |A|^m$$

για κάθε $t \in TT^{-1}$.

Απόδειξη. Ξεκινάμε όπως στην απόδειξη της Πρότασης 4.2.5, θεωρώντας ένα τυχαίο υποσύνολο C του A πληθαρίθμου k, όπου το k θα επιλεγεί κατάλληλα. Σταθεροποιούμε ένα στοιχείο $x \in G$. Όπως έχουμε εξηγήσει, η τυχαία μεταβλητή $\mathbf{1}_C * \mathbf{1}_B(x)$ έχει υπεργεωμετρική κατανομή: πιο συγκεκριμένα,

$$\mathbb{P}(\mathbf{1}_C * \mathbf{1}_B(x) = j) = \binom{M}{j}\binom{|A| - M}{k - j}\Big/\binom{|A|}{k},$$

όπου $M := \mathbf{1}_A * \mathbf{1}_B(x) = |A \cap xB^{-1}|$. Η πιθανότητα είναι ακριβώς το ποσοστό των k-συνόλων C στο A τα οποία περιέχουν ακριβώς j στοιχεία του $A \cap xB^{-1}$. Από το Λήμμα 4.2.6 έχουμε ότι

$$\mathbb{E}\left|\mathbf{1}_C * \mathbf{1}_B(x) - \frac{k}{|A|}\mathbf{1}_A * \mathbf{1}_B(x)\right|^{2m} \leqslant 2(3mk \cdot \mathbf{1}_A * \mathbf{1}_B(x)/|A| + m^2)^m,$$

και χρησιμοποιώντας την $\mu_C := \frac{|A|}{k}\mathbf{1}_C$ παίρνουμε

$$\mathbb{E}\,|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)|^{2m} \leqslant 2(m|A|/k)^m(3 \cdot \mathbf{1}_A * \mathbf{1}_B(x) + m|A|/k)^m.$$

Αθροίζοντας πάνω από όλα τα $x \in A \cdot B$ έχουμε ότι

$$\mathbb{E}\,\|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant 2(m|A|/k)^m \sum_{x \in A \cdot B}(3 \cdot \mathbf{1}_A * \mathbf{1}_B(x) + m|A|/k)^m.$$

Συμβολίζουμε το δεξιό μέλος αυτής της ανισότητας με λ. Από την ανισότητα Markov βλέπουμε τότε ότι

$$\mathbb{P}\left(\|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant 2\lambda\right) \geqslant \frac{1}{2}.$$

Η συνέχεια της απόδειξης είναι τώρα εντελώς ανάλογη με αυτήν στην απόδειξη της Πρότασης 4.2.5. Αντικαθιστούμε την L^2-προσέγγιση που χρησιμοποιήσαμε εκεί με την L^{2m}-προσέγγιση που έχουμε εδώ. Βρίσκουμε έτσι ένα σύνολο $C \subseteq S \cdot A$ πληθαρίθμου k με την ιδιότητα ότι το σύνολο

$$T := \{t \in S^{-1} : \|\mu_C * \mathbf{1}_B(x) - \mathbf{1}_A * \mathbf{1}_B(tx)\|_{2m}^{2m} \leqslant \lambda\}$$

έχει πληθάριθμο τουλάχιστον $|S|/(2K)^k$. Το αποτέλεσμα προκύπτει τώρα από την τριγωνική ανισότητα αν παρατηρήσουμε ότι ισχύει η ανισότητα

$$\lambda \leqslant 2(m|A|/k)^m 3.05^m \max\{\|\mathbf{1}_A * \mathbf{1}_B\|_m, 20m|AB|\,|A|/k)^m$$

και επιλέξουμε $k := \lfloor 49m/\varepsilon \rfloor$. □

4.3 Η δομή των συνόλων γινομένων

Σε αυτή την ενότητα παρουσιάζουμε μη-μεταθετικά ανάλογα της θεωρίας των Bogolyubov, Freiman, Halberstam, Ruzsa σχετικά με τη δομή συνόλων αθροισμάτων. Ένα γενικό πρόβλημα της προσθετικής συνδυαστικής είναι να αποδειχθούν ποσοτικά αποτελέσματα για τη δομή συνόλων αθροισμάτων σε αβελιανές ομάδες. Ένα κλασικό θεώρημα αυτού του τύπου είναι το θεώρημα του Bogolyubov, το οποίο ισχυρίζεται ότι αν ένα σύνολο A έχει μικρό τετράγωνο τότε το $2A - 2A$ έχει συγκεκριμένη δομή. Ένα ανάλογο αυτού του θεωρήματος για μη-αβελιανές ομάδες αποδείχθηκε από τον Sanders.

Θεώρημα 4.3.1 (Sanders). *Έστω G μια ομάδα και A πεπερασμένο υποσύνολο της G τέτοιο ώστε $|A^2| \leqslant K|A|$. Για κάθε $k \geqslant 1$ υπάρχει συμμετρικό σύνολο S που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $S^k \subseteq A^1 \cdot A^{-2}$ και*

$$|S| \geqslant \exp(-K^{O(k)})|A|.$$

Τα θεωρήματα σχεδόν περιοδικότητας της προηγούμενης παραγράφου είναι πολύ κατάλληλα ως εργαλεία για την απόδειξη αποτελεσμάτων όπως το Θεώρημα 4.3.1 και μάλιστα με πολύ καλές εκτιμήσεις. Πράγματι, χρησιμοποιώντας την Πρόταση 4.2.1 θα δείξουμε το εξής.

Θεώρημα 4.3.2. *Έστω G μια ομάδα και A πεπερασμένο υποσύνολο της G τέτοιο ώστε $|A^2| \leqslant K|A|$. Για κάθε $k \geqslant 1$ υπάρχει συμμετρικό σύνολο $S \subseteq A^{-1}A$ που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $S^k \subseteq A^1 \cdot A^{-2}$ και*

$$|S| \geqslant \exp(-9k^2 K \log(2K))|A|.$$

Επιπλέον, κάθε στοιχείο του S^k έχει τουλάχιστον $|A|^3/2K$ αναπαραστάσεις της μορφής $a_1 a_2 a_3^{-1} a_4^{-1}$ με $a_i \in A$.

Απόδειξη. Θέτουμε $\varepsilon := 1/k\sqrt{K}$ και εφαρμόζοντας την Πρόταση 4.2.5 για το A με $B = S = A$ παίρνουμε ένα σύνολο $T \subseteq A^{-1}$ με πληθάριθμο μεγαλύτερο ή ίσο από $|A|/(2K)^{9k^2K}$ τέτοιο ώστε

$$\|\mathbf{1}_A * \mathbf{1}_A(tx) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2^2 \leqslant \varepsilon^2 |A|^3$$

για κάθε $t \in TT^{-1}$. Θέτουμε $S := TT^{-1}$. Από την τριγωνική ανισότητα έπεται ότι

$$\|\mathbf{1}_A * \mathbf{1}_A(tx) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2^2 \leqslant |A|^3/K$$

για κάθε $t \in S^k$. Αναπτύσσοντας το αριστερό μέλος αυτής της ανισότητας παίρνουμε

$$2\sum_{x\in G} \mathbf{1}_A * \mathbf{1}_A(x)^2 - 2\sum_{x\in G} \mathbf{1}_A * \mathbf{1}_A(tx)\mathbf{1}_A * \mathbf{1}_A(x)$$
$$= 2(E(A,A) - \mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_{A^{-1}} * \mathbf{1}_{A^{-1}}(t)).$$

Αφού το A έχει μικρό τετράγωνο, από την (4.1.4) έχει μεγάλη πολλαπλασιαστική ενέργεια. Έχουμε

$$E(A,A) \geqslant |A|^3/K.$$

Συνεπώς,

$$\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_{A^{-1}} * \mathbf{1}_{A^{-1}}(t) \geqslant |A|^3(1/K - 1/(2K)) = |A|^3/2K.$$

Αφού η $\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_{A^{-1}} * \mathbf{1}_{A^{-1}}$ έχει φορέα το $A^2 \cdot A^{-2}$, συμπεραίνουμε ότι $S^k \subseteq A^2 \cdot A^{-2}$ όπως θέλαμε. Επιπλέον, κάθε στοιχείο $t \in S^k$ έχει, λόγω της (4.1.1), πολλές αναπαραστάσεις ως γινόμενο της μορφής $a_1a_2a_3^{-1}a_4^{-1}$ με $a_i \in A$. $\square$

Η ακόλουθη γενικότερη έκδοση του Θεωρήματος 4.3.2 αποδεικνύεται με τον ίδιο περίπου τρόπο.

Θεώρημα 4.3.3. *Έστω G μια ομάδα, A, B πεπερασμένα μη κενά υποσύνολα της G, και $k \geqslant 1$. Υποθέτουμε ότι $E(A,B) \geqslant |A|^2|B|/K$ και ότι $|D \cdot A| \leqslant K'|A|$ για κάποιο σύνολο $D \subseteq G$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq D^{-1}D$ που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $S^k \subseteq A \cdot B \cdot B^{-1} \cdot A^{-1}$ και*

$$|S| \geqslant \exp(-9k^2K\log(2K'))|D|.$$

Επιπλέον, κάθε στοιχείο του S^k έχει τουλάχιστον $|A|^2|B|/2K$ αναπαραστάσεις της μορφής $a_1b_1b_2^{-1}a_2^{-1}$ με $a_i \in A$, $b_i \in B$.

Με κάποια πρόσθετη προσπάθεια μπορούμε να αποδείξουμε ένα αποτέλεσμα που ισχύει για σύνολα τριπλών γινομένων. Για να το διατυπώσουμε είναι βολικό να εισαγάγουμε την ακόλουθη ορολογία: Για μια τριάδα (A, B, C) πεπερασμένων υποσυνόλων της G και ένα στοιχείο $x \in G$ λέμε ότι το x είναι γ-δημοφιλές αν

$$\mathbf{1}_A * \mathbf{1}_B * \mathbf{1}_C(x) \geqslant \gamma(|A|\,|B|)^{1/2}|C|.$$

Με άλλα λόγια, το x είναι γ-δημοφιλές αν γράφεται ως γινόμενο abc όπου $a \in A$, $b \in B$, $c \in C$ με τουλάχιστον $\gamma(|A|\,|B|)^{1/2}|C|$ διαφορετικούς τρόπους. Αν ο πληθάριθμος $|A \cdot B \cdot C|$ είναι μικρός τότε υπάρχει σίγουρα κάποιο δημοφιλές στοιχείο, αφού

$$|A|\,|B|\,|C| = \sum_{x \in A\cdot B\cdot C} \mathbf{1}_A * \mathbf{1}_B * \mathbf{1}_C(x) \leqslant |A \cdot B \cdot C| \sup_{x\in G} \mathbf{1}_A * \mathbf{1}_B * \mathbf{1}_C(x),$$

υπάρχουν όμως πολύ ασθενέστερες συνθήκες που εξασφαλίζουν το ίδιο πράγμα. Μία τέτοια συνθήκη είναι η

$$E(A,B) \geqslant |A|^2|B|/K$$

διότι $E(A,B) = \mathbf{1}_A * \mathbf{1}_B * \mathbf{1}_{B^{-1}} * \mathbf{1}_{A^{-1}}(1)$ και από την αρχή του περιστερώνα έπεται ότι αν η πολλαπλασιαστική ενέργεια $E(A,B)$ είναι μεγάλη τότε υπάρχει δημοφιλές στοιχείο για την τριάδα (B, B^{-1}, A^{-1}).

Θεώρημα 4.3.4. *Έστω G μια ομάδα, A_1, A_2, A_3 πεπερασμένα μη κενά υποσύνολα της G και $k \geqslant 1$. Έστω x ένα $\frac{1}{K}$-δημοφιλές στοιχείο της τριάδας (A_1, A_2, A_3) και D ένα υποσύνολο της G τέτοιο ώστε $|A_3 \cdot D| \leqslant K'|A_3|$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq DD^{-1}$ που περιέχει το ταυτοτικό στοιχείο της G τέτοιο ώστε $xS^k \subseteq A_1A_2A_3$ και*

$$|S| \geqslant \exp(-36k^2K^2\log(2K'))|D|.$$

Απόδειξη. Από την υπόθεση έχουμε

$$\mathbf{1}_{A_1} * \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(x) \geqslant (|A_1|\,|A_2|)^{1/2}|A_3|/K$$

και $|A_3 \cdot D| \leqslant K'|A_3|$. Εφαρμόζουμε την Πρόταση 4.2.1 για τα σύνολα $A = A_2$ και $B = A_3$ με $\varepsilon := 1/(2kK)$ και παίρνουμε ένα σύνολο $T \subseteq D$ με πληθάριθμο τουλάχιστον $|D|/(2K')^{36k^2K^2}$ τέτοιο ώστε

$$\|\mathbf{1}_{A_2} * \mathbf{1}_{A_3}(yt) - \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(y)\|_2^2 \leqslant \varepsilon^2|A_2|\,|A_3|^2$$

για κάθε $t \in S := TT^{-1}$. Έτσι, για κάθε $t \in S^k$ έχουμε

$$\|\mathbf{1}_{A_2} * \mathbf{1}_{A_3}(yt) - \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(y)\|_2^2 \leqslant \frac{1}{4K^2}|A_2|\,|A_3|^2.$$

Έστω $t \in S^k$. Εφαρμόζοντας την ανισότητα Cauchy-Schwarz παίρνουμε

$$\begin{aligned}
&|\mathbf{1}_{A_1} * \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(xt) - \mathbf{1}_{A_1} * \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(x)| \\
&\qquad = \left|\sum_{y\in G} \mathbf{1}_{A_1}(y)(\mathbf{1}_{A_2} * \mathbf{1}_{A_3}(y^{-1}xt) - \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(y^{-1}x))\right| \\
&\qquad \leqslant |A_1|^{1/2}\|\mathbf{1}_{A_2} * \mathbf{1}_{A_3}(yt) - \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(y)\|_2.
\end{aligned}$$

Έπεται ότι

$$|\mathbf{1}_{A_1} * \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(xt) - \mathbf{1}_{A_1} * \mathbf{1}_{A_2} * \mathbf{1}_{A_3}(x)| \leqslant \frac{1}{2K}(|A-1|\,|A_2|)^{1/2}|A_3|.$$

Αφού το x είναι $\frac{1}{K}$-δημοφιλές στοιχείο της G και το $t \in S^k$ ήταν τυχόν, η απόδειξη είναι πλήρης. $\square$

Στην περίπτωση του γινομένου δύο συνόλων η κατάσταση μοιάζει διαφορετική. Παρόλο που δεν μπορούμε να εξασφαλίσουμε ότι υπάρχει μεταφορά ενός μεγάλου συνόλου διαδοχικών γινομένων στο $A \cdot B$, μπορούμε πάντοτε να βρούμε μια μεταφορά οποιουδήποτε μικρού υποσυνόλου ενός μεγάλου συνόλου διαδοχικών γινομένων.

Θεώρημα 4.3.5. *Έστω G μια ομάδα, A, B πεπερασμένα μη κενά υποσύνολα της G και $k, n \geqslant 1$ δύο παράμετροι. Υποθέτουμε ότι $|A \cdot B| \leqslant K|A|$ και $|B \cdot D| \leqslant K'|B|$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq DD^{-1}$ με πληθάριθμο*

$$|S| \geqslant \exp(-150k^2 K \log(2K') \log(2n))|D|$$

τέτοιο ώστε το σύνολο γινομένων $A \cdot B$ να περιέχει μία αριστερή μεταφορά οποιουδήποτε συνόλου $P \subseteq S^k$ που έχει πληθάριθμο μικρότερο ή ίσο από n.

Το Θεώρημα 4.3.5 είναι ειδική περίπτωση του ακόλουθου αποτελέσματος, το οποίο έχει το πλεονέκτημα ότι δίνει ισχυρότερα αποτελέσματα στην περίπτωση που ο πληθάριθμος $|A \cdot B|$ δεν είναι μικρός αλλά η πολλαπλασιαστική ενέργεια $E(A, B)$ εξακολουθεί να είναι μεγάλη.

Θεώρημα 4.3.6. *Έστω G μια ομάδα, A, B πεπερασμένα μη κενά υποσύνολα της G και $k, n \in \mathbb{N}$ δύο παράμετροι. Υποθέτουμε ότι:*

- $E(A, B) \geqslant |A|\,|B|^2/K_1$,
- $|A \cdot B| \leqslant K_2|A|$ *και*
- $|B \cdot S| \leqslant K_3|B|$.

Τότε υπάρχει ένα σύνολο $T \subseteq S$ με πληθάριθμο

$$|T| \geqslant \exp(-150k^2(K_1K_2)^{1/2}(\log(2K_3))(\log(2n)))|S|$$

τέτοιο ώστε το σύνολο γινομένων $A \cdot B$ να περιέχει μια αριστερή μεταφορά οποιουδήποτε συνόλου $P \subseteq (TT^{-1})^k$ που έχει πληθάριθμο μικρότερο ή ίσο από n.

Απόδειξη. Μπορούμε να υποθέσουμε ότι $n \geqslant 2$. Θέτουμε $m := \log(2n)$, ορίζουμε μια σταθερά γ μέσω της

$$\|\mathbf{1}_A * \mathbf{1}_B\|_m^m = \gamma^m |AB|\,|B|^m$$

και θέτουμε $\varepsilon := \gamma/ek^2$. Εφαρμόζοντας την Πρόταση 4.2.3 για τά σύνολα A και B με αυτές τις παραμέτρους βρίσκουμε ένα σύνολο $T \subseteq S$ με

$$|T| \geqslant \frac{|S|}{(2K_3)^{50ek^2(\log 2n)/\gamma}}$$

τέτοιο ώστε
$$\|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \leqslant \varepsilon^m |B|^m \|\mathbf{1}_A * \mathbf{1}_B\|_m^m$$
για κάθε $t \in TT^{-1}$. Έστω $P \subseteq (TT^{-1})^k$ ένα σύνολο με πληθάριθμο μικρότερο ή ίσο από n. Υποθέτουμε, προς άτοπο, ότι το $A \cdot B$ δεν περιέχει καμία αριστερή μεταφορά του P. Τότε για κάθε $x \in G$ υπάρχει στοιχείο $t \in P$ τέτοιο ώστε $xt \notin A \cdot B$, δηλαδή τέτοιο ώστε
$$\mathbf{1}_A * \mathbf{1}_B(xt) = 0.$$

Συνεπώς,
$$\begin{aligned} nk^{2m}\varepsilon^m |B|^m \|\mathbf{1}_A * \mathbf{1}_B\|_m^m &\geqslant \sum_{t \in P} \|\mathbf{1}_A * \mathbf{1}_B(xt) - \mathbf{1}_A * \mathbf{1}_B(x)\|_{2m}^{2m} \\ &\geqslant \sum_{x \in G} \mathbf{1}_A * \mathbf{1}_B(x)^{2m} \\ &\geqslant \|\mathbf{1}_A * \mathbf{1}_B\|_m^{2m} / |AB| \end{aligned}$$
από την ανισότητα Cauchy-Schwarz. Από τον ορισμό των ε και m οδηγούμαστε τώρα σε άτοπο. Άρα, υπάρχει x τέτοιο ώστε $xP \subseteq A \cdot B$. Τώρα, έπεται το ζητούμενο αν παρατηρήσουμε ότι $\gamma \geqslant 1/(K_1K_2)^{1/2}$, το οποίο είναι συνέπεια της ανισότητας Hölder και της (4.1.3). □

Στην περίπτωση που ο πληθάριθμος $|A \cdot B|$ δεν είναι μικρός συγκρινόμενος με τον $|A|$, το συμπέρασμα του θεωρήματος είναι πολύ ασθενέστερο. Αν ικανοποιείται η συνθήκη $E(A, B) \geqslant |A|\,|B|^2/K$ για την ενέργεια και αν τα A και B έχουν το ίδιο περίπου μέγεθος, τότε μπορούμε να εφαρμόσουμε το θεώρημα Balog-Szemerédi-Gowers και να βρούμε μεγάλα υποσύνολα $A' \subseteq A$ και $B' \subseteq B$ στα οποία κατόπιν να εφαρμόσουμε το θεώρημα. Έτσι παίρνουμε καλύτερα φράγματα από αυτά που θα προέκυπταν αν χρησιμοποιούσαμε απευθείας κάποια μεγάλη τιμή της σταθεράς K_3.

4.4 Δομημένα σύνολα μεταφορών

Η Πρόταση 4.2.1 και η Πρόταση 4.2.3 μας δίνουν πολύ μεγάλα σύνολα μεταφορών για τα οποία η $\mathbf{1}_A * \mathbf{1}_B$ είναι σχεδόν αναλλοίωτη ως προς μεταφορές. Συχνά όμως χρειαζόμαστε τα σύνολα αυτά να είναι ταυτόχρονα δομημένα. Για παράδειγμα, στις εφαρμογές που θα δώσουμε για την αβελιανή πππερίπτωση, θέλουμε να μπορούμε να βρούμε αριθμητικές προόδους αυτών των μεταφορών. Με τις μεθόδους της Ανάλυσης Fourier η ύπαρξη μιας αριθμητικής προόδου σχεδόν-περιόδων προκύπτει συνήθως εύκολα διότι παίρνουμε ένα σύνολο Bohr τέτοιων μεταφορών. Όμως εδώ δεν έχουμε αυτή τη δυνατότητα. Θα προσπαθήσουμε λοιπόν να παράξουμε τη δομή με επαναλαμβανόμενη πρόσθεση συνόλων.

Λέμε ότι μια αριθμητική πρόοδος P σε μια αβελιανή ομάδα έχει μήκος k αν μπορεί να γραφτεί ως

$$P = \{a, a+d, \ldots, a+(k-1)d\}$$

για κάποιο μη μηδενικό στοιχείο d.

Λήμμα 4.4.1. *Έστω G μια αβελιανή ομάδα, $S \subseteq G$ ένα πεπερασμένο υποσύνολο που ικανοποιεί την $|S+S| \leqslant K|S|$ ή την $|S-S| \leqslant K|S|$, και $k \in \mathbb{N}$. Υποθέτουμε ότι το $A \subseteq S$ ικανοποιεί την $|A| \geqslant \delta|S|$, όπου*

$$\delta > K^{3k/2}/|S|^{1/(k+1)}.$$

Τότε το σύνολο $kA - kA$ περιέχει μια συμμετρική αριθμητική πρόοδο που έχει μήκος τουλάχιστον 2^{k+1}, περνάει από το 0, και έχει μη-μηδενικό βήμα $d \in A - A$.

Για την απόδειξη χρειαζόμαστε το επόμενο απλό λήμμα. Το λήμμα δεν μας χρειάζεται όταν $K = 1$, που ισχύει στην περίπτωση που το X είναι ομάδα.

Λήμμα 4.4.2. *Έστω G μια αβελιανή ομάδα και $A \subseteq G$ ένα πεπερασμένο υποσύνολο που ικανοποιεί την $|A+A| \leqslant K|A|$ ή την $|A-A| \leqslant K|A|$. Έστω $k \in \mathbb{N}$. Τότε*

$$|A - 2^k \cdot A| \leqslant K^{3k}|A|.$$

Απόδειξη. Από την τριγωνική ανισότητα του Ruzsa (Λήμμα 4.1.1) έχουμε ότι

$$|A - 2^k \cdot A| \leqslant \frac{|A - 2\cdot A|\,|2\cdot A - 2^k \cdot A|}{|A|} \leqslant \frac{|A - 2\cdot A|\,|A - 2^{k-1}\cdot A|}{|A|}.$$

Άρα,

$$\frac{|A - 2^k \cdot A|}{|A|} \leqslant \left(\frac{A - 2\cdot A|}{|A|}\right)^k.$$

Το λήμμα έπεται τώρα από την ειδική περίπτωση $|A - 2\cdot A| \leqslant K^3|A|$ της ανισότητας Plünnecke-Ruzsa (Θεώρημα 4.1.2). □

Απόδειξη του Λήμματος 4.4.1. Αρκεί να δείξουμε ότι υπάρχουν διακεκριμένα στοιχεία $a, b \in A$ τέτοια ώστε

$$2^j(a-b) \in A - A \quad \text{για κάθε } j = 1, \ldots, k,$$

αφού τότε, παίρνοντας δυαδικά αναπτύγματα, συμπεραίνουμε ότι

$$[-2^k, 2^k] \cdot (a-b) \subseteq kA - kA.$$

Ισοδύναμα, αρκεί να δείξουμε ότι υπάρχουν διακεκριμένα $a, b \in A$ και $x_j, y_j \in A$ τέτοια ώστε

$$\begin{aligned} x_1 - 2a &= y_1 - 2b \\ x_2 = 4a &= y_2 - 4b \\ &\vdots \\ x_k - 2^k a &= y_k - 2^k b. \end{aligned}$$

Θα δείξουμε ότι αυτό το σύστημα εξισώσεων έχει λύση με $a \neq b$. Πράγματι, για κάθε $(k+1)$-άδα στοιχείων $(a, x_1, \ldots, x_k) \in A^{k+1}$, θέτουμε

$$f(a, x_1, \ldots, x_k) := (x_1 - 2a, x_2 - 4a, \ldots, x_k - 2^k a).$$

Η εικόνα αυτής της συνάρτησης είναι ένα υποσύνολο του $(S - 2 \cdot S) \times \cdots \times (S - 2^k \cdot S)$, το οποίο, από το Λήμμα 4.4.2 έχει πληθάριθμο μικρότερο ή ίσο από $K^{3k(k+1)/2}|S|^k$. Αν λοιπόν $|A|^{k+1} > K^{3k(k+1)/2}|S|^k$, το οποίο ισχύει λόγω του φράγματος που έχουμε υποθέσει για το δ, πρέπει να υπάρχουν δύο διακεκριμένες $(k+1)$-άδες $\mathbf{a} = (a, x_1, \ldots, x_k)$ και $\mathbf{b} = (b, y_1, \ldots, y_k)$ στο A^{k+1} τέτοιες ώστε $f(\mathbf{a}) = f(\mathbf{b})$. Αναγκαστικά έχουμε $a \neq b$, συνεπώς έχουμε βρει μια μη-τετριμμένη λύση για το σύστημά μας. □

Συνδυάζοντας το Λήμμα 4.4.1 και την Πρόταση 4.2.1 παίρνουμε το ακόλουθο πόρισμα, το οποίο θα μας φανεί χρήσιμο στην απόδειξη του θεωρήματος του Roth.

Πόρισμα 4.4.3. *Έστω $\delta \in (0,1)$ και $A \subseteq [N]$ με πληθάριθμο αN, όπου $\alpha \geqslant 4N^{-\delta^2/36}$. Τότε υπάρχει συμμετρική αριθμητική πρόοδος $P \subseteq [-N/2, N/2]$ μήκους*

$$|P| \geqslant \exp\left(\frac{1}{14}\left(\frac{\delta^2 \log N}{\log 4/\alpha}\right)^{1/3}\right)$$

τέτοια ώστε $0 \in P$ και, για κάθε $t \in P$,

$$\|\mathbf{1}_A * \mathbf{1}_A(x+t) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2^2 \leqslant \delta^2 |A|^3.$$

Απόδειξη. Θέτουμε

$$k := \left\lfloor \left(\frac{\delta^2 \log n}{36 \log 4/\alpha}\right)^{1/3} \right\rfloor$$

και

$$\varepsilon := \delta/k,$$

και εφαρμόζουμε την Πρόταση 4.2.1 για το A με $B = A$ και $S = [N]$. Παρατηρήστε ότι μπορούμε να επιλέξουμε $K = 2/\alpha$ διότι $A + [N] \subseteq [2N]$. Παίρνουμε έτσι ένα σύνολο $T \subseteq [N]$ με πληθάριθμο τουλάχιστον ίσο με $(\alpha/4)^{9/\varepsilon^2} N$, το οποίο ικανοποιεί την

$$\|\mathbf{1}_A * \mathbf{1}_A(x+t) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2^2 \leqslant \varepsilon^2 |A|^3$$

για κάθε $t \in T - T$. Εφαρμόζοντας το Λήμμα 4.4.1 για το σύνολο T παίρνουμε μια συμμετρική αριθμητική πρόοδο $P \subseteq kT - kT$ που έχει μήκος τουλάχιστον ίσο με $2^{k+1} + 1$. Από την τριγωνική ανισότητα έχουμε τότε ότι για κάθε $t \in T$ ισχύει

$$\|\mathbf{1}_A * \mathbf{1}_A(x+t) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2^2 \leqslant \delta^2 |A|^3.$$

Αυτή η αριθμητική πρόοδος θα ικανοποιούσε το συμπέρασμα του πορίσματος, με την διαφορά ότι δεν γνωρίζουμε αν περιέχεται στο $[-N/2, N/2]$. Περιέχεται όμως στο $[-kN, kN]$. Μπορούμε λοιπόν να επιλέξουμε μια συμμετρική υπο-πρόοδο $P' \subseteq [-N/2, N/2]$ της P η οποία να έχει μήκος μεγαλύτερο ή ίσο από $2\lfloor 2^{k-1}/k \rfloor + 1$. Αυτή η πρόοδος μας δίνει το ζητούμενο. Παρατηρήστε ότι η συνθήκη για το α προέρχεται από τον περιορισμό ότι το k πρέπει να είναι τουλάχιστον ίσο με 1. □

4.5 Αριθμητικές πρόοδοι σε σύνολα αθροισμάτων

Αφετηρία των αποτελεσμάτων αυτής της ενότητας είναι ένα θεώρημα του Bourgain ο οποίος, χρησιμοποιώντας ανάλυση Fourier στο $\mathbb{Z}_p$, απέδειξε ότι αν A και B είναι υποσύνολα του $[N]$ με πυκνότητα α και β αντίστοιχα, τότε το $A + B$ πρέπει να περιέχει μια αριθμητική πρόοδο μήκους τουλάχιστον

$$\exp(c((\alpha\beta \log N)^{1/3} - \log\log N))$$

όπου $c > 0$ είναι μια απόλυτη σταθερά. Στη συνέχεια αυτό το κάτω φράγμα βελτιώθηκε από τον Green, και ανεξάρτητα από τον Sanders, οι οποίοι πέτυχαν τον εκθέτη $1/2$ αντί του $1/3$.

Συνδυάζοντας το Θεώρημα 4.3.6, το οποίο είναι συνέπεια της Πρότασης 4.2.3, με το Λήμμα 4.4.1 παίρνουμε το εξής.

Θεώρημα 4.5.1. *Έστω N ένας θετικός ακέραιος και $A, B \subseteq [N]$ μη κενά σύνολα με πληθάριθμο αN και βN αντίστοιχα. Τότε το $A + B$ περιέχει μια αριθμητική πρόοδο μήκους τουλάχιστον*

$$\frac{1}{2}\exp\left(c\left(\frac{\alpha \log N}{\log 4/\beta}\right)^{1/4}\right)$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Το Θεώρημα 4.5.1, συγκρινόμενο με τα αποτελέσματα των Bourgain, Green και Sanders, δίνει αριθμητικές προόδους μικρότερου μήκους όταν τα σύνολα έχουν μεγάλη πυκνότητα (το οποίο σημαίνει ότι οι σταθερές α και β δεν εξαρτώνται από το N), εφαρμόζεται όμως και για πολύ μικρότερα σύνολα και καλύπτει περιπτώσεις που τα προηγούμενα αποτελέσματα δεν μπορούσαν να αντιμετωπίσουν. Για να εφαρμόσουμε τα προηγούμενα αποτελέσματα κατά μη τετριμμένο τρόπο θα πρέπει να ισχύει ότι $\alpha\beta \geqslant C(\log\log N)^2/\log N$ ενώ μπορούμε να εφαρμόσουμε το Θεώρημα 4.5.1 αν υποθέσουμε ότι $\alpha(\log 4/\beta)^{-1} \geqslant C/\log N$. Μας επιτρέπει έτσι να μελετήσουμε ζευγάρια συνόλων καθένα από τα οποία έχει πυκνότητα μεγαλύτερη ή ίση από $C\log\log N/\log N$ ενώ για να εφαρμόσουμε τα προηγούμενα αποτελέσματα θα πρέπει τουλάχιστον ένα από τα σύνολα να έχει πυκνότητα μεγαλύτερη ή ίση από $C\log\log N/(\log N)^{1/2}$. Ένα άλλο καινούργιο σημείο της μεθόδου που χρησιμοποιείται εδώ είναι ότι μπορούμε να δουλέψουμε απευθείας με την ομάδα $\mathbb{Z}$ και δεν χρειάζεται να εμβαπτίσουμε τα σύνολα σε κάποια ομάδα $\mathbb{Z}_p$ όπως συνηθίζεται κατά την εφαρμογή μεθόδων της ανάλυσης Fourier.

Απόδειξη του Θεωρήματος 4.5.1. Θέτουμε

$$k := \Big\lfloor \frac{1}{10}\Big(\frac{\alpha\log N}{\log 4/\beta}\Big)^{1/4}\Big\rfloor$$

και

$$n := 2^{k+1}.$$

Υποθέτουμε ότι $k \geqslant 1$, αλλιώς το συμπέρασμα του θεωρήματος ισχύει κατά τετριμμένο τρόπο. Εφαρμόζουμε το Θεώρημα 4.3.6 για τα A και B με αυτές τις παραμέτρους και με $S = [N]$. Αφού

$$A + B \subseteq B + [N] \subseteq [2N]$$

μπορούμε να επιλέξουμε $K_2 = 2/\alpha$ και $K_3 = 2/\beta$, και μπορούμε να πάρουμε $K_1 = K_2$ λόγω της (4.1.4). Έτσι παίρνουμε ένα σύνολο $T \subseteq [N]$ με πληθάριθμο δN, όπου

$$\delta \geqslant \exp(-300k^2(\log 4/\beta)(\log 2n)/\alpha),$$

με την ιδιότητα ότι το $A+B$ περιέχει μεταφορά οποιουδήποτε υποσυνόλου P του $kT - kT$ το οποίο έχει πληθάριθμο το πολύ ίσο με n. Από το Λήμμα 4.4.1 μπορούμε να βρούμε μια αριθμητική πρόοδο P μήκους n στο $kT - kT$ αρκεί να ικανοποιείται η συνθήκη

$$\delta \geqslant 2^{3k/2}/N^{1/(k+1)},$$

η οποία ελέγχουμε ότι ικανοποιείται, με απλές πράξεις. □

Παρατήρηση 4.5.2. Όπως έχουμε ήδη αναφέρει, σε αντίθεση με προηγούμενες αποδείξεις αποτελεσμάτων της ίδιας μορφής με το Θεώρημα 4.5.1, δεν χρειάστηκε να εμβαπτίσουμε τα σύνολα A και B σε κάποια πεπερασμένη ομάδα $\mathbb{Z}_p$ για κάποιον πρώτο p μεγαλύτερο από N, ώστε να συνεχίσουμε εκεί τους υπολογισμούς μας. Αν όμως το είχαμε κάνει, θα μπορούσαμε να είχαμε χρησιμοποιήσει μια ελαφρώς απλούστερη μορφή του Λήμματος 4.4.1 γιατί θα μας χρειαζόταν να το χρησιμοποιήσουμε μόνο με $K = 1$.

Με μια απλή τροποποίηση της απόδειξης της Πρότασης 4.2.10, χρησιμοποιώντας την τριγωνική ανισότητα για να απαλλαγούμε από τους όρους $\mathbf{1}_A * \mathbf{1}_B(x)$ αντί για τους όρους $\mu_C * \mathbf{1}_B(x)$, μπορούμε να συμπεράνουμε ότι $P \subseteq A+C$ για ένα πολύ μικρό σύνολο $C \subseteq B$. Έτσι, χρειάζεται να μεταφέρουμε το A κατά πολύ λίγα στοιχεία του B για να δημιουργήσουμε αριθμητικές προόδους μεγάλου μήκους.

Με τον ιδιο τρόπο παίρνουμε την ακόλουθη τοπική εκδοχή του Θεωρήματος 4.5.1.

Θεώρημα 4.5.3 (αριθμητικές πρόοδοι σε μικρά σύνολα αθροισμάτων)**.** *Έστω A και B πεπερασμένα μη κενά υποσύνολα μιας αβελιανής ομάδας, τέτοια ώστε*

$$|A+B| \leqslant K_1|A| \qquad \text{και} \qquad |A+B| \leqslant K_2|B|.$$

Τότε το $A+B$ περιέχει αριθμητική πρόοδο μήκους τουλάχιστον ίσου με

$$\frac{1}{2}\exp\left(c\left(\frac{\log|A|}{K_1\log 2K_2}\right)^{1/4}\right),$$

όπου $c>0$ είναι μια απόλυτη σταθερά.

Απόδειξη. Η απόδειξη είναι ουσιαστικά ίδια με την προηγούμενη. Θέτουμε

$$k := \left\lfloor \frac{1}{10}\Big(\frac{\log|A|}{K_1\log 2K_2}\Big)^{1/4}\right\rfloor$$

και $n := 2^{k+1}$. Όπως πριν, εφαρμόζουμε το Θεώρημα 4.3.6 για τα A και B με αυτές τις παραμέτρους, όμως αυτή τη φορά παίρνουμε $S=A$. Έτσι, βρίσκουμε $T \subseteq A$ με πληθάριθμο

$$|T| \geqslant \exp(-150k^2K_1(\log 2K_2)(\log 2n))|A|$$

τέτοιο ώστε το $A+B$ να περιέχει όλα τα υποσύνολα του $kT-kT$ που έχουν πληθάριθμο μικρότερο ή ίσο από n. Από την ανισότητα Plünnecke-Ruzsa (Θεώρημα 4.1.2) έπεται ότι

$$|A+A| \leqslant K_1K_2^2|A|.$$

Ένας απλός υπολογισμός δείχνει ότι μπορούμε να εφαρμόσουμε το Λήμμα 4.4.1 για το $T \subseteq A$ και να βρούμε μια αριθμητική πρόοδο μήκους n στο $kT-kT$, το οποίο μας δίνει το ζητούμενο αν $k \geqslant 1$ (παρατηρήστε ότι το θεώρημα πάλι ισχύει τετριμμένα αν $k<1$). □

Παρατήρηση 4.5.4. Σημειώνουμε ότι οι αριθμητικές πρόοδοι μπορεί να είναι εκφυλισμένες σε κάποιες ομάδες, όπως για παράδειγμα η ομάδα $\mathbb{F}_2^n$.

Μπορούμε να αποδείξουμε και άλλες τοπικές εκδοχές αυτού του αποτελέσματος. Για παράδειγμα, θα μπορούσαμε να δουλέψουμε με κάποιο S που έχει μικρό τετράγωνο, τέτοιο ώστε $|B+S| \leqslant K|B|$. Αυτό θα οδηγούσε σε λίγο καλύτερες εκτιμήσεις.

Κλείνουμε αυτή την παράγραφο αναφέροντας μια αξιοσημείωτη κατασκευή του Ruzsa, η οποία δείχνει ότι υπάρχουν κάποια όρια στο πόσο ισχυρά αποτελέσματα της παραπάνω μορφής θα μπορούσε να περιμένει κανείς.

Θεώρημα 4.5.5 (Ruzsa). *Έστω $\varepsilon > 0$. Για κάθε πρώτο $p > p_0(\varepsilon)$ υπάρχει ένα συμμετρικό σύνολο $A \subseteq \mathbb{Z}_p$ με πληθάριθμο μεγαλύτερο ή ίσο από $(1/2-\varepsilon)p$ τέτοιο ώστε το $A+A$ να μην περιέχει αριμητική πρόοδο μήκους*

$$\exp((\log p)^{2/3+\varepsilon}).$$

Σημειώνουμε επίσης ότι αν κάποιος θέλει να βρει αριθμητικές προόδους μήκους της τάξης του $\log N$ στο $A+B$ τότε υπάρχουν ισχυρότερα αποτελέσματα. Αποτελέσματα των Croot, Ruzsa και Schoen δείχνουν ότι μπορεί κανείς να δουλέψει με σύνολα πολύ πιο αραιά από αυτά που συζητήσαμε εδώ.

4.6 Το θεώρημα του Roth

Σε αυτή την ενότητα μελετάμε και πάλι την ποσότητα $R(N)$, το μέγιστο πλήθος που μπορεί να έχει ένα υποσύνολο του $[N] = \{1, \dots, N\}$ το οποίο δεν περιέχει καμία αριθμητική πρόοδο τριών όρων, δηλαδή δεν περιέχει τριάδα $(x, x+d, x+2d)$ με $d \neq 0$. Χρησιμοποιώντας την πιθανοθεωρητική απόδειξη της Πρότασης 4.2.1 μπορούμε να δώσουμε καθαρά συνδυαστική απόδειξη της ακόλουθης εκδοχής του θεωρήματος του Roth.

Θεώρημα 4.6.1. *Υπάρχει συνάρτηση ω με $\omega(N) \to \infty$ όταν $N \to \infty$ τέτοια ώστε*

$$R(N) \leqslant \frac{N}{(\log\log N)^{\omega(N)}}$$

για κάθε φυσικό αριθμό N.

Το φράγμα για την $R(N)$ στο Θεώρημα 4.6.1 είναι ελαφρώς καλύτερο από το αρχικό φράγμα

$$R(N) \ll \frac{N}{\log\log N}$$

του Roth. Μεταγενέστερα επιχειρήματα, με μεθόδους ανάλυσης Fourier, οδήγησαν σε καλύτερα φράγματα για την $R(N)$. Ο Bourgain έχει αποδείξει ότι

$$R(N) \ll \frac{(\log\log N)^2}{(\log N)^{2/3}} N.$$

Υπάρχουν αρκετές αποδείξεις του θεωρήματος του Roth, μερικές από τις οποίες δεν χρησιμοποιούν ανάλυση Fourier. Όμως μόνο αυτές που χρησιμοποιούν ανάλυση Fourier δίνουν εκτιμήσεις αυτής της τάξης. Εκείνες οι αποδείξεις που αποφεύγουν την ανάλυση Fourier δίνουν μόνο φράγματα της μορφής

$$R(N) \ll N/\log^* N,$$

όπου $\log^* N$, ο επαναλαμβανόμενος λογάριθμος του N είναι ο μικρότερος φυσικός k που απαιτείται ώστε αν πάρουμε k φορές διαδοχικά λογάριθμο του N να πάρουμε αριθμό μικρότερο ή ίσο από 1. Αυτό λοιπόν που είναι ενδιαφέρον στην απόδειξη που θα δώσουμε εδώ είναι ότι επιτυγχάνει φράγματα αντίστοιχα με αυτά που δίνουν οι μέθοδοι της ανάλυσης Fourier παρόλο που αποφεύγει την χρήση ανάλυσης Fourier.

Η στρατηγική που θα ακολουθήσουμε για την απόδειξη του Θεωρήματος 4.6.1 είναι η «αύξηση της πυκνότητας». Θα δείξουμε ότι αν κάποιο $A \subseteq \{1,\dots,N\}$ είναι μεγάλο και δεν περιέχει αριθμητικές προόδους μήκους 3 τότε μπορούμε να βρούμε μια μεγάλη αριθμητική πρόοδο πάνω στην οποία το A έχει σημαντικά μεγαλύτερη πυκνότητα. Μπορούμε μετά να επαναλάβουμε αυτό το επιχείρημα αρκετές φορές ώστε να καταλήξουμε σε αντίφαση.

Για την απόδειξη θα χρειαστεί να εισαγάγουμε κάποιο συμβολισμό. Συμβολίζουμε με $T_3(f)$ το άθροισμα μια συνάρτησης $f : \mathbb{Z} \to \mathbb{R}$ με πεπερασμένο φορέα πάνω από όλες τις αριθμητικές προόδους τριών όρων στο $\mathbb{Z}$. Δηλαδή,

$$T_3(f) := \sum_{x,y\in\mathbb{Z}} f(x)f(y)f(2y-x) = \sum_{y\in\mathbb{Z}} f(y)(f*f)(2y).$$

Αν $f = \mathbf{1}_A$ είναι η δείκτρια συνάρτηση ενός συνόλου τότε η ποσότητα $T_3(f)$ δίνει το πλήθος των αριθμητικών προόδων μήκους 3 στο A. Σημειώνουμε ότι με αυτό τον τρόπο συμπεριλαμβάνονται οι τετριμμένες, δηλαδή σταθερές, αριθμητικές πρόοδοι και μετράμε την $(x, x+d, x+2d)$ ως διαφορετική από την $(x+2d, x+d, x)$. Συμβολίζουμε με μ_X την κανονικοποιημένη δείκτρια συνάρτηση $\mathbf{1}_X/|X|$ ενός πεπερασμένου συνόλου X. Για ένα υποσύνολο A του X θα λέμε ότι το A έχει πυκνότητα α ως προς X αν $|A| = \alpha|X|$.

Πρόταση 4.6.2. *Έστω $\varepsilon > 0$ και έστω ότι το $A \subseteq [N]$ έχει πληθάριθμο αN. Τότε υπάρχει μια συμμετρική αριθμητική πρόοδος $P \subseteq [-N/8, N/8]$ που έχει μήκος τουλάχιστον*

$$|P| \geqslant c\exp\left(c\left(\frac{\varepsilon^2\log N}{\log(4/\alpha)}\right)^{1/3}\right),$$

όπου $c > 0$ είναι μια απόλυτη σταθερά, τέτοια ώστε

$$|T_3(\mathbf{1}_A * \mu_P) - T_3(\mathbf{1}_A)| \leqslant \varepsilon|A|^2.$$

Απόδειξη. Έστω Q η αριθμητική πρόοδος που παίρνουμε αν εφαρμόσουμε το Πόρισμα 4.4.3 στο A με παράμετρο ε^2. Η Q είναι μεγάλη, επίσης $Q = -Q$ και $Q \subseteq [-N/2, N/2]$. Έστω P μια συμμετρική υπο-πρόοδος της Q με μήκος μεγαλύτερο ή ίσο από $|Q|/8$, τέτοια ώστε

$4P \subseteq Q$, οπότε $P \subseteq [-N/8, N/8]$. Θα δείξουμε ότι η P ικανοποιεί το συμπέρασμα της πρότασης. Πράγματι,

$$T_3(\mathbf{1}_A * \mu_P) = \mathbb{E}_{(y,z,w)\in P^3} \sum_x \mathbf{1}_A(x)\mathbf{1}_A * \mathbf{1}_A(2x + 2y - z - w)$$

άρα

$$\begin{aligned} |T_3(\mathbf{1}_A * \mu_P) - T_3(\mathbf{1}_A)| &= |\mathbb{E}_{y,z,w\in P} \sum_x \mathbf{1}_A(x)(\mathbf{1}_A * \mathbf{1}_A(2x + 2y - z - w) - \mathbf{1}_A * \mathbf{1}_A(2x))| \\ &\leqslant |A|^{1/2}\mathbb{E}_{z,w\in P, y\in 2\cdot P}\|\mathbf{1}_A * \mathbf{1}_A(x - y - z - w) - \mathbf{1}_A * \mathbf{1}_A(x)\|_2 \\ &\leqslant \varepsilon|A|^2, \end{aligned}$$

από την τριγωνική ανισότητα, την ανισότητα Cauchy-Scwarz και το γεγονός ότι $P + P + 2 \cdot P \subseteq Q$ □

Θα χρειαστούμε επίσης ένα λήμμα για την T_3 το οποίο δίνει κάτω φράγμα για το ε-λάχιστο πλήθος αριθμητικών προόδων τριών όρων που μπορεί να περιέχει ένα σύνολο ή μια συνάρτηση, αν έχουμε κάποια άνω φράγματα για τη συνάρτηση R. Είναι μια ποσοτική εκδοχή ενός επιχειρήματος του Varnavides.

Λήμμα 4.6.3 (το θεώρημα του Varnavides)**.** *Έστω N ένας φυσικός αριθμός και $f : [N] \to [0, 1]$ μια συνάρτηση με μέση τιμή*

$$\mathbb{E}_{x\in[N]} f(x) = \alpha.$$

Τότε, για κάθε θετικό ακέραιο $M \leqslant N^{1/10}/2$,

$$T_3(f) \geqslant \left(\alpha - \frac{R(M) + 2}{M}\right) M^{-4}N^2.$$

Η απόδειξη αυτού του λήμματος βασίζεται σε μια τεχνική διπλού μετρήματος. Η απόδειξη για την περίπτωση $f = \mathbf{1}_A$ μπορεί να βρεθεί σε προηγούμενη εργασία των Croot και Sisask. Για να περάσουμε στο γενικό αποτέλεσμα, για μια συνάρτηση f, μπορούμε να χρησιμοποιήσουμε ένα συνηθισμένο πιθανοθεωρητικό τέχνασμα: ορίζουμε ένα τυχαίο υποσύνολο A του $[N]$ θέτοντας $x \in A$ με πιθανότητα $f(x)$ ανεξάρτητα για κάθε x. Οι λεπτομέρειες υπάρχουν στο βιβλίο των Tao και Vu.

Μπορούμε τώρα να αποδείξουμε το Θεώρημα 4.6.1 στην εξής ισοδύναμη μορφή.

Θεώρημα 4.6.4. *Για κάθε $c > 0$ υπάρχουν θετικοί αριθμοί C και N_0 τέτοιοι ώστε*

$$R(N) \leqslant CN/(\log\log N)^c$$

για κάθε $N \geqslant N_0$.

Απόδειξη. Έστω A ένα υποσύνολο του $\{1,\dots,N\}$ με πληθάριθμο $\alpha N = R(N)$ το οποίο δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων και έστω $\varepsilon > 0$ μία παράμετρος που θα επιλέξουμε αργότερα. Εφαρμόζοντας την Πρόταση 4.6.2 για το A παίρνουμε μια μεγάλη αριθμητική πρόοδο P τέτοια ώστε

$$|T_3(\mathbf{1}_A * \mu_P) - T_3(\mathbf{1}_A)| \leqslant \varepsilon |A|^2. \tag{4.6.1}$$

Θα μελετήσουμε τη συνάρτηση

$$\mathbf{1}_A * \mu_P(x) = |A \cap (x-P)|/|P|.$$

Θα δείξουμε ότι αν επιλέξουμε κατάλληλο $0 < \delta < 1$ τότε υπάρχει x τέτοιο ώστε

$$|A \cap (x-P)| > \delta^{-1}\alpha |P|.$$

Αυτή η ανισότητα θα μας επιτρέψει να εφαρμόσουμε το επιχείρημα αύξησης της πυκνότητας.

Έστω ότι $\mathbf{1}_A * \mu_P(x) \leqslant \delta^{-1}\alpha$ για κάθε $x \in \mathbb{Z}$. Ορίζουμε $f(x) := (\delta/\alpha)\mathbf{1}_A * \mu_P(x)$. Τότε, $0 \leqslant f(x) \leqslant 1$ για κάθε x, $\sum_x f(x) = \delta N$, και

$$T_3(f) = (\delta/\alpha)^3 T_3(\mathbf{1}_A * \mu_P).$$

Παρατηρούμε επίσης ότι ο φορέας της f περιέχεται στο $A + P \subseteq [1 - N/8, 9N/8] \cap \mathbb{Z}$, που είναι διάστημα μήκους $5N/4$. Το A περιέχει μόνο τετριμμένες αριθμητικές προόδους τριών όρων, άρα $T_2(\mathbf{1}_A) = |A|$. Από την (4.6.1) έπεται ότι

$$T_3(f) \leqslant 2\delta^3 \varepsilon N^2/\alpha \tag{4.6.2}$$

αν υποθέσουμε ότι $\varepsilon \geqslant 1/|A|$. Από την άλλη πλευρά, λόγω του Λήμματος 4.6.3 έχουμε

$$T_3(f) \geqslant \Big(\frac{4}{5}\delta - \frac{R(M)+2}{M}\Big) M^{-4} N^2$$

αν υποθέσουμε ότι $M \leqslant N^{1/10}/2$.

Αρχικά επιλέγουμε $\delta = 9/10$. Μπορούμε εύκολα να ελέγξουμε ότι $R(10) = 5$. Επιλέγοντας λοιπόν $<= 10$ βλέπουμε ότι $T_3(f) \geqslant c_0 N^2$ για κάποια θετική απόλυτη σταθερά c_0. Συγκρίνοντας με την (4.6.2) βλέπουμε ότι θα καταλήξουμε σε άτοπο αν επιλέξουμε $\varepsilon = c_1\alpha$ για κάποια μικρή σταθερά $c_1 > 0$. Αυτό γίνεται αν υποθέσουμε ότι $\alpha \geqslant 1/\sqrt{c_1 N}$. Έπεται ότι

$$|A \cap (x-P)| \geqslant \frac{10}{9}\alpha |P|$$

για κάποιον ακέραιο x, όπου P είναι μια μεγάλη αριθμητική πρόοδος. Υποθέτουμε ότι $\alpha \geqslant (\log N)^{-1/6}$. Τότε

$$|P| \geqslant \exp((\log N)^{1/8}).$$

Καταλήγουμε έτσι στο ότι το A έχει πυκνότητα τουλάχιστον $\frac{10}{9}\left(\frac{R(N)}{N}\right)$ σε μια αριθμητική πρόοδο μήκους $N_1 := |P|$. Κάνοντας αλλαγή κλίμακας παίρνουμε ένα σύνολο $A_1 \subseteq \{1, \ldots, N_1\}$ το οποίο επίσης δεν περιέχει αριθμητικές προόδους, είναι όμως τώρα πολύ πιο πυκνό άπό το αρχικό σύνολο A.

Μπορούμε τώρα να επαναλάβουμε αυτό το επιχείρημα, παίρνοντας μια ακολουθία φυσικών N_j με

$$N_j \geqslant \exp((\log N_{j-1})^{1/8})$$

και μια ακολουθία πυκνοτήτων δ_j με

$$\delta_j \geqslant \left(\frac{10}{9}\right)^j \left(\frac{R(N)}{N}\right).$$

Οι μόνες προϋποθέσεις για να μπορούμε να κάνουμε το επόμενο βήμα αυτής της διαδικασίας είναι να ισχύουν οι $\delta_j \geqslant (\log N_j)^{-1/8}$ και $N_j \geqslant C$ για κάποια απόλυτη σταθερά C. Αφού κανένας δ_j δεν είναι μεγαλύτερος από 1, αυτή η διαδικασία πρέπει να σταματήσει σε κάποιο βήμα K με

$$K \leqslant \frac{\log(N/R(N))}{\log(10/9)},$$

και σε αυτό το σημείο κάποια από τις προϋποθέσεις δεν ικανοποιείται. Συμπεραίνουμε έτσι ότι

$$R(N) \leqslant \frac{CN}{(\log\log N)^{\frac{\log 10/9}{\log 8}}}$$

για κάποια απόλυτη σταθερά C.

Έχουμε έτσι αποδείξει το θεώρημα για κάποιον σταθερό εκθέτη c του $\log\log N$. Μπορούμε τώρα, χρησιμοποιώντας αυτό το συμπέρασμα, να επαναλάβουμε το επιχείρημα, με τη διαφορά ότι τώρα δεν χρειαζόμαστε κάποιους περιορισμούς για να εφαρμόσουμε το Λήμμα 4.6.3. Δηλαδή, μπορούμε τώρα να επιλέξουμε δ οσοδήποτε μικρό και να βρούμε μια σταθερά M που ικανοποιεί την

$$\frac{4}{5}\delta - \frac{R(M)+2}{M} \geqslant \frac{\delta}{2}.$$

Αυτό σημαίνει ότι, αντί να πάρουμε αύξηση πυκνότητας ίση με $\frac{10}{9}$, μπορούμε να επιτύχουμε αύξηση ίση με οσοδήποτε μεγάλο παράγοντα $\frac{1}{\delta}$, πάλι πάνω σε μια πρόοδο που έχει μήκος τουλάχιστον $\exp((\log N)^{1/8})$, μόνο που τώρα πρέπει το N να είναι αρκετά μεγάλο σαν συνάρτηση του δ. Με το επιχείρημα που χρησιμοποιήσαμε προηγουμένως, βλέπουμε ότι

$$R(N) \leqslant \frac{CN}{(\log\log N)^{\frac{\log \delta^{-1}}{\log 8}}}$$

για $N \geqslant N_0(\delta)$ και κάποια σταθερά που εξαρτάται από το δ. $\square$

4.7 Ισχυρές προσεγγιστικές ομάδες

Κλείνουμε αυτό το κεφάλαιο με μια τελευταία εφαρμογή της πιθανοθεωρητικής τεχνικής των Croot και Sisask. Η επόμενη πρόταση δείχνει ότι τα γινόμενα συνόλων που «μοιάζουν με ομάδες» έχουν αναγκαστικά ισχυρές ιδιότητες σχεδόν περιοδικότητας.

Πρόταση 4.7.1. *Έστω A ένα πεπερασμένο υποσύνολο μιας ομάδας και έστω $\varepsilon \in (0,1)$. Υποθέτουμε ότι το A έχει την ιδιότητα ότι κάθε $x \in A^2$ έχει τουλάχιστον $|A|/K$ αναπαραστάσεις της μορφής ab με $a, b \in A$. Τότε υπάρχει συμμετρικό σύνολο $S \subseteq A^{-1}A$ με πληθάριθμο*

$$|S| \geqslant \exp(-K^2 \log(2K) \log(8/\varepsilon))|A|$$

τέτοιο ώστε, για κάθε $t \in S$,

$$|tA^2 \triangle A^2| \leqslant \varepsilon |A^2|.$$

Ο Green αποκαλεί τα σύνολα A που ικανοποιούν την υπόθεση αυτής της πρότασης «ισχυρές K-προσεγγιστικές ομάδες». Δηλαδή, το A είναι ισχυρή K-προσεγγιστική ομάδα αν $\mathbf{1}_A * \mathbf{1}_A(x) \geqslant |A|/K$ για κάθε $x \in A^2$. Προφανώς, κάθε υποομάδα μιας ομάδας είναι ισχυρή K-προσεγγιστική ομάδα με $K = 1$, υπάρχουν όμως κι άλλα, πιο πολύπλοκα, παραδείγματα. Αν $p > 3$ είναι ένας πρώτος αριθμός ισότιμος με τον $3 \pmod 4$ τότε το σύνολο $A \subseteq \mathbb{Z}_p$ που αποτελείται από τα μη μηδενικά τετράγωνα είναι ισχυρή $\left(\frac{1}{2} - o(1)\right)$-προσεγγιστική ομάδα, διότι $A + A = \mathbb{Z}_p \setminus \{0\}$ και $\mathbf{1}_A * \mathbf{1}_A(x) \geqslant \left(\frac{1}{2} - o(1)\right)|A|$ για κάθε μη μηδενικό $x \in \mathbb{Z}_p$. Σημειώνουμε επίσης ότι αν $A \subseteq G$ και $B \subseteq H$ είναι δύο ισχυρές K_A- και K_B-προσεγγιστικές ομάδες τότε το $A \times B \subseteq G \times H$ είναι ισχυρή $K_A K_B$-προσεγγιστική ομάδα.

Η Πρόταση 4.7.1 δεν είναι άμεση συνέπεια των θεωρημάτων της σχεδόν περιοδικότητας. Η απόδειξή της όμως χρησιμοποιεί τις ιδέες που υπάρχουν στις αποδείξεις αυτών των θεωρημάτων με έναν λίγο διαφορετικό τρόπο.

Απόδειξη της Πρότασης 4.7.1. Θα αποδείξουμε ότι αν επιλέξουμε τυχαίο $C \subseteq A$ τότε $CA \approx A^2$ με αρκετά μεγάλη πιθανότητα. Πράγματι, ξεκινάμε επιλέγοντας τυχαίο σύνολο $C \subseteq A$ με πληθάριθμο k. Από την υπόθεση για το A, κάθε $x \in A^2$ το οποίο ικανοποιεί την

$$|\mu_C * \mathbf{1}_A(x) - \mathbf{1}_A * \mathbf{1}_A(x)| < |A|/K$$

βρίσκεται στο CA, άρα

$$\mathbb{P}(x \notin CA) \leqslant \mathbb{P}(|\mu_C * \mathbf{1}_A(x) - \mathbf{1}_A * \mathbf{1}_A(x)| \geqslant |A|/K) \leqslant 2e^{-2k/K^2}.$$

Η τελευταία ανισότητα είναι γνωστή για την υπεργεωμετρική κατανομή (βλ. και την Πρόταση 4.2.9). Αθροίζοντας πάνω από όλα τα $x \in A^2$ παίρνουμε

$$\mathbb{E}|\{x \in Ar : x \notin CA\}| \leqslant 2e^{-2k/K^2}|A^2|.$$

Από την ανισότητα Markov έπεται ότι

$$\mathbb{P}(|A^2 \triangle CA| \leqslant \lambda |A^2|) \geqslant 1 - 2e^{-2k/K^2}/\lambda,$$

και αν επιλέξουμε $\lambda := 4e^{-2k/K^2}$ μπορούμε να κάνουμε αυτή την πιθανότητα μεγαλύτερη ή ίση από $1/2$.

Παρατηρούμε τώρα ότι $|A^2| \leqslant K|A|$. Αυτό προκύπτει από την ανισότητα

$$\mathbf{1}_A * \mathbf{1}_A(x) \geqslant |A|\, \mathbf{1}_{A^2}(x)/K$$

η οποία ισχύει για κάθε x. Όπως στην απόδειξη της Πρότασης 4.2.5, αυτό σημαίνει ότι υπάρχουν ένα σύνολο C και ένα σύνολο $T \subseteq A^{-1}$ με πληθάριθμο μεγαλύτερο ή ίσο από $|A|/(2K)^k$ ώστε

$$|A^2 \triangle tCA| \leqslant \lambda |A^2|$$

για κάθε $t \in T$. Επομένως, για κάθε $t_1, t_2 \in T$ έχουμε

$$|t_2 t_1^{-1} A^2 \triangle A^2| \leqslant 2\lambda |A^2|$$

από την τριγωνική ανισότητα. Επιλέγοντας $k := \lceil (K^2 \log(8/\varepsilon)/2 \rceil$ και $S := TT^{-1}$ ολοκληρώνουμε την απόδειξη. □

Παρατήρηση 4.7.2. Είναι εύκολο να δούμε ότι μια ισχυρή K-προσεγγιστική ομάδα πρέπει να έχει μικρό τετράγωνο: ισχύει η ανισότητα $|A^2| \leqslant K|A|$. Σε αντίθεση όμως με τα σύνολα που έχουν μικρό τετράγωνο, δεν είναι σαφές πόσο πολλές είναι οι ισχυρές K-προσεγγιστικές ομάδες δοθέντος πληθαρίθμου, ακόμα και μέσα στην ομάδα $\mathbb{Z}_p$ όπου p πρώτος. Ο Konyagin έχει θέσει το βασικό ερώτημα αν για κάθε σύνολο $A \subseteq \mathbb{Z}_p$ με πληθάριθμο μικρότερο από $\sqrt{p}$ υπάρχει κάποιο στοιχείο $x \in A + A$ τέτοιο ώστε

$$\mathbf{1}_A * \mathbf{1}_A(x) \leqslant C|A|^{1-c},$$

όπου $C, c > 0$ είναι απόλυτες σταθερές. Από τη δουλειά των Luczak και Schoen, καθώς και από τη δουλειά των Green και Ruzsa, είναι γνωστό ότι μπορεί κανείς πάντα να βρει $x \in A + A$ τέτοιο ώστε

$$\mathbf{1}_A * \mathbf{1}_A(x) \leqslant \max\{1, |A|/(\log_2 p)^{1/2+o(1)}\}.$$

Τα αποτελέσματα αυτού του κεφαλαίου οδηγούν σε φράγματα παρόμοια με αυτό.

ΚΕΦΑΛΑΙΟ 5

Η εκτίμηση των Bloom και Sisask

5.1 Το θεώρημα των Bloom και Sisask

Κλείνουμε αυτή την εργασία με μια περιγραφή του ακόλουθου πολύ πρόσφατου θεωρήματος των Bloom και Sisask.

Θεώρημα 5.1.1 (Bloom-Sisask). *Έστω $N \geqslant 2$ και $A \subseteq \{1, \ldots, N\}$ σύνολο που δεν περιέχει μη τετριμμένες αριθμητικές προόδους τριών όρων, δηλαδή λύσεις της $x + y = 2z$ με $x \neq y$. Τότε*

$$|A| \ll \frac{N}{(\log n)^{1+c}},$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Έχουμε ήδη δει ότι καλύτερο γνωστό φράγμα πριν από αυτό το θεώρημα των Bloom και Sisask ήταν $N/(\log n)^{1-o(1)}$. Υπήρχαν τρεις διαφορετικές αποδείξεις αυτής της εκτίμησης, μία του Sanders, μία του Bloom και μία των Bloom και Sisask, με ελαφρώς διαφορετική συμπεριφορά του $o(1)$ όρου. Μία ακόμη καλύτερη εκτίμηση, της ίδιας όμως μορφής, είχε δοθεί από τον Schoen, ο οποίος συνδύασε το τελευταίο επιχείρημα των Bloom και Sisask με κάποιες ιδέες των Bateman και Katz.

Είναι η πρώτη φορά που δίνεται φράγμα $o(N/\log N)$ για το πρόβλημα. Όλες οι προηγούμενες απόπειρες δεν είχαν κατορθώσει να σπάσουν το φράγμα $1/\log N$ για την πυκνότητα του A.

Το Θεώρημα 5.1.1 βρίσκει εφαρμογή σε μια πολύ γνωστή εικασία του Erdős που ισχυρίζεται ότι αν A είναι ένα σύνολο φυσικών αριθμών τέτοιο ώστε η σειρά $\sum\limits_{n \in A} \frac{1}{n}$ να αποκλίνει τότε το A περιέχει αριθμητικές προόδους οσοδήποτε μεγάλου μήκους. Ως πόρισμα του Θεωρήματος 5.1.1 παίρνουμε την πρώτη μη τετριμμένη περίπτωση αυτής της εικασίας.

Πόρισμα 5.1.2. *Έστω $A \subseteq \mathbb{N}$ τέτοιο ώστε $\sum_{n\in A} \frac{1}{n} = \infty$. Τότε το A περιέχει άπειρες το πλήθος μη τετριμμένες αριθμητικές προόδους τριών όρων.*

Απόδειξη. Υποθέτουμε ότι το A περιέχει πεπερασμένες το πλήθος αριθμητικές προόδους τριών όρων. Τότε, για κάθε N,

$$F(N) := |A \cap \{1, \ldots, N\}| \ll \frac{N}{(\log N)^{1+c}} + 1,$$

όπου $c > 0$ είναι η σταθερά του Θεωρήματος 5.1.1. Αθροίζοντας κατά μέρη παίρνουμε

$$\sum_{n\in A\cap[N]} \frac{1}{n} = \frac{F(N)}{N} + \int_1^N \frac{F(t)}{t^2}\, dt \ll \int_1^N \frac{1}{t(\log t)^{1+c}}\, dt + 1 \ll 1.$$

Αφήνοντας το $N \to \infty$ συμπεραίνουμε ότι η σειρά $\sum_{n\in A} \frac{1}{n}$ συγκλίνει. □

Έχοντας ξεπεράσει το φράγμα $1/\log N$ για την πυκνότητα, μπορούμε επίσης να βρούμε αριθμητικές προόδους τριών όρων στους πρώτους χρησιμοποιώντας απλώς την εκτίμηση του Chebyshev ότι το πλήθος των πρώτων στο $\{1, \ldots, N\}$ είναι $\gg N/\log N$. Για παράδειγμα, παίρνουμε άμεσα μια ισχυρή μορφή ενός θεωρήματος του Green: κάθε υποσύνολο των πρώτων με θετική σχετική πυκνότητα, περιέχει άπειρες το πλήθος μη τετριμμένες αριθμητικές προόδους τριών όρων. Μάλιστα, χρησιμοποιώντας απλώς την εκτίμηση του Chebyshev, παίρνουμε το εξής:

Πόρισμα 5.1.3. *Έστω $\mathbb{P}$ το σύνολο των πρώτων και έστω $A \subset \mathbb{P} \cap \{1, \ldots, N\}$. Αν το A δεν έχει μη τετριμμένες αριθμητικές προόδους τριών όρων τότε το A έχει σχετική πυκνότητα*

$$\frac{|A|}{|\mathbb{P} \cap \{1, \ldots, N\}|} \ll \frac{1}{(\log N)^c}$$

για κάποια απόλυτη σταθερά $c > 0$.

5.2 Προκαταρκτικά αποτελέσματα

Σε ό,τι ακολουθεί, G είναι μια πεπερασμένη αβελιανή ομάδα περιττής τάξης N, οποία στις εφαρμογές μας θα είναι η $\mathbb{Z}_N$. Η δυϊκή ομάδα $\widehat{G}$ είναι η ομάδα των προσθετικών χαρακτήρων της G, η οποία είναι μια πεπερασμένη αβελιανή ομάδα ισόμορφη με την G. Χρησιμοποιούμε την πρόσθεση για να συμβολίζουμε την πράξη της ομάδας τόσο στην G όσο και στην $\widehat{G}$. Για παράδειγμα, αν $\gamma_1, \gamma_2 : G \to \mathbb{C}$ είναι δύο χαρακτήρες στην $\widehat{G}$ τότε

$$(\gamma_1 + \gamma_2)(x) = \gamma_1(x)\gamma_2(x).$$

Για κάθε συνάρτηση $f : G \to \mathbb{C}$ και κάθε μη κενό $X \subset G$ γράφουμε $\mathbb{E}_{x\in X} f(x)$ για τον μέσο όρο $|X|^{-1} \sum_{x\in X} f(x)$. Συνήθως θεωρούμε την περίπτωση $X = G$ και τότε γράφουμε $\mathbb{E}_x$ αντί για $\mathbb{E}_{x\in G}$. Οι L^p-νόρμες στην G θεωρούνται με αυτή την κανονικοποίηση, ενώ στην $\widehat{G}$ με το μέτρο απαρίθμησης. Δηλαδή, αν $f : G \to \mathbb{C}$ και $1 \leqslant p < \infty$ θέτουμε

$$\|f\|_p = (\mathbb{E}_x |f(x)|^p)^{1/p} \quad \text{και} \quad \|f\|_\infty = \sup_{x\in G} |f(x)|$$

και αν $\omega : \widehat{G} \to \mathbb{C}$ θέτουμε

$$\|\omega\|_p = \left(\sum_{\gamma\in\widehat{G}} |\omega(\gamma)|^p \right)^{1/p} \quad \text{και} \quad \|\omega\|_\infty = \sup_{\gamma\in\widehat{G}} |\omega(\gamma)|.$$

Όμοια, τα εσωτερικά γινόμενα και οι συνελίξεις ορίζονται με τις κατάλληλες κανονικοποιήσεις, ανάλογα με το αν οι συναρτήσεις είναι ορισμένες στην G ή στην $\widehat{G}$. Για παράδειγμα, αν $f, g : G \to \mathbb{C}$ τότε

$$\langle f, g\rangle = \mathbb{E}_x f(x)\overline{g(x)}.$$

Ειδικότερα, για κάθε $f : G \to \mathbb{C}$ ο μετασχηματισμός Fourier $\widehat{f} : \widehat{G} \to \mathbb{C}$ ορίζεται από την

$$\widehat{f}(\gamma) = \mathbb{E}_x f(x)\overline{\gamma(x)}.$$

Με αυτές τις κανονικοποιήσεις, η ταυτότητα Parseval ισχυρίζεται ότι για κάθε $f, g : G \to \mathbb{C}$

$$\langle f, g\rangle = \langle \widehat{f}, \widehat{g}\rangle.$$

Θα χρησιμοποιούμε συχνά το συμβολισμό $f \circ g$ για την $f * g_-$, όπου $g_-(x) = g(-x)$. Αυτή η πράξη δεν είναι γενικά προσεταιριστική, ικανοποιεί όμως την $(f\circ g)\circ h = f\circ(g\circ h_-)$, άρα αν η h είναι συμμετρική τότε ισχύει η προσεταιριστική ιδιότητα και παραλείπουμε τις παρενθέσεις. Γράφουμε $f^{(n)}$ για την n-οστή επαναλαμβανόμενη συνέλιξη. Θα χρησιμοποιούμε συχνά τις στοιχειώδεις ιδιότητες

$$\widehat{f * g} = \widehat{f} \cdot \widehat{g} \quad \text{και} \quad \widehat{f \circ g} = \widehat{f} \cdot \overline{\widehat{g}}.$$

Ένα μέτρο πιθανότητας είναι μια μη αρνητική συνάρτηση $\mu : G \to \mathbb{R}^+$ τέτοια ώστε $\|\mu\|_1 = 1$.

Θα χρησιμοποιούμε επίσης τον αντίστροφο μετασχηματισμό Fourier, ο οποίος ορίζεται για συναρτήσεις $\omega : \widehat{G} \to \mathbb{C}$ από την

$$\check{\omega}(x) = \sum_{\gamma\in\widehat{G}} \omega(\gamma)\gamma(x).$$

Αν $A \subset B$, τότε ονομάζουμε τον λόγο $|A|/|B|$ πυκνότητα του A ως προς το (ή στο) B. Συνήθως γράφουμε $\alpha = |A|/|B|$ για την πυκνότητα του A στο B, όπου $A \subset B \subset G$. Συμβολίζουμε με μ το ομοιόμορφο μέτρο στην G, δηλαδή αν $B \subset G$ έχουμε $\mu(B) =$

$\|\mathbf{1}_B\|_1 = |B|/N$. Γράφουμε μ_B για την κανονικοποιημένη δείκτρια συνάρτηση $\mu(B)^{-1}\mathbf{1}_B$ και για το μέτρο $\mu_B(A) = |A \cap B|/|B|$. Θέτουμε επίσης

$$\mu_{A/B} = \mu_A - \mu_B = (\alpha^{-1}\mathbf{1}_A - \mathbf{1}_B)\mu(B)^{-1}.$$

Παρατηρούμε ότι

$$\|\mu_{A/B}\|_1 = 2(1-\alpha) \quad \text{και} \quad \|\mu_{A/B}\|_2^2 = \mu(B)^{-1}(\alpha^{-1}-1).$$

Ειδικότερα, αν $0 < \alpha \leqslant 1/2$ έχουμε $\|\mu_{A/B}\|_1 \approx 1$ και $\|\mu_{A/B}\|_2^2 \approx \alpha^{-1}\mu(B)^{-1}$.

Θα χρησιμοποιούμε συχνά την δυαδική αρχή του περιστερώνα. Παραδείγματα αποτελεσμάτων αυτού του τύπου, τα οποία θα χρησιμοποιούμε ελεύθερα αναφερόμενοι στη «δυαδική αρχή του περιστερώνα» δίνουν τα επόμενα δύο λήμματα.

Λήμμα 5.2.1. *Έστω $f : X \to [0, M]$ και $0 < \delta \leqslant 1$ τέτοια ώστε*

$$\sum_{x\in X} f(x) \geqslant \delta M|X|.$$

Τότε υπάρχουν $\delta/2 \leqslant \eta \leqslant 1$ και $X' \subset X$ με πληθάριθμο $|X'| \succeq_\delta \delta\eta^{-1}|X|$ τέτοια ώστε αν $x \in X'$ τότε $2\eta M > f(x) \geqslant \eta M$.

Απόδειξη. Έστω $\tilde{X} = \{x \in X : f(x) \geqslant \frac{1}{2}\delta M\}$. Από την υπόθεση,

$$\sum_{x\in\tilde{X}} f(x) = \sum_{x\in X} f(x) - \sum_{x\notin\tilde{X}} f(x) \geqslant \frac{1}{2}\delta M|X|.$$

Ορίζουμε

$$X_i = \{x \in \tilde{X} : 2^{i-1}\delta M \leqslant f(x) < 2^i\delta M\}.$$

Τα σύνολα X_i είναι ξένα και το X_i είναι κενό αν $i > \log_2(2/\delta)$ ή $i < 0$. Από την αρχή του περιστερώνα υπάρχει κάποιος $0 \leqslant i \leqslant \log_2(2/\delta)$ τέτοιος ώστε

$$\sum_{x\in X_i} f(x) \geqslant \frac{\delta}{2\lceil\log_2(2/\delta)+1\rceil}M|X|.$$

Τώρα το ζητούμενο έπεται αν θέσουμε $X' = X_i$ και $\eta = 2^{i-1}\delta$. □

Με πολύ παρόμοιο τρόπο δείχνουμε την ακόλουθη εναλλακτική μορφή του προηγούμενου λήμματος.

Λήμμα 5.2.2. *Έστω $f : X \to [0, M]$ και $0 < \delta \leqslant 1$ τέτοια ώστε*

$$\sum_{x\in X} f(x)^2 \geqslant \delta M \sum_{x\in X} f(x).$$

Τότε υπάρχουν $1 \geqslant \eta \geqslant \delta/2$ και $X' \subset X$ με πληθάριθμο

$$|X'| \succeq_\delta \delta\eta^{-2}M^{-1}\sum_{x\in X} f(x)$$

ώστε $2\eta M > f(x) \geqslant \eta M$ για κάθε $x \in X'$.

5.3 Περιγραφή της απόδειξης

Στόχος μας είναι να δώσουμε άνω φράγμα για το πλήθος των συνόλων A με λίγες λύσεις της $x + y = 2z$ (για παράδειγμα, αυτά για τα οποία οι μόνες λύσεις είναι οι $|A|$ το πλήθος τετριμμένες για τις οποίες $x = y = z$). Για το σκοπό αυτό θα αποδείξουμε ένα κάτω φράγμα για το πλήθος των λύσεων σε τυχόν σύνολο δεδομένης πυκνότητας. Θα θεωρήσουμε την ποσότητα

$$T(A) = \mathbb{E}_{x,d}\mathbf{1}_A(x)\mathbf{1}_A(x+d)\mathbf{1}_A(x+2d) = \mathbb{E}_{x,y}\mathbf{1}_A(x)\mathbf{1}_A(y)\mathbf{1}_{2\cdot A}(x+y)$$

που μετράει (κανονικοποιημένα) το πλήθος των αριθμητικών προόδων μήκους 3 (συμπεριλαμβανομένων των τετριμμένων) στο A. Δείχνουμε τώρα το εξής:

Θεώρημα 5.3.1. *Αν G είναι μια πεπερασμένη αβελιανή ομάδα με περιττή τάξη και $A \subset G$ με πυκνότητα α τότε*

$$T(A) \geqslant \exp(-O(\alpha^{-1+c})),$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Δεδομένου ότι αν ένα σύνολο περιέχει μόνο τετριμμένες αριθμητικές προόδους μήκους 3 τότε $T(A) = \alpha/N$, παίρνουμε το εξής πόρισμα.

Πόρισμα 5.3.2. *Έστω G μια πεπερασμένη αβελιανή ομάδα με περιττή τάξη και $A \subset G$ με πυκνότητα α. Τότε,*

$$T(A) \gg \exp(-O(\alpha^{-1+c}))$$

όπου $c > 0$ είναι μια απόλυτη σταθερά.

Το Θεώρημα 5.1.1 προκύπτει άμεσα από αυτό το αποτέλεσμα αν εμφυτεύσουμε το $\{1, \dots, N\}$ στο $\mathbb{Z}_{N'}$ όπου $N' = 2N + 1$, οπότε κάθε αριθμητική πρόοδος τριών όρων στην εικόνα του $\{1, \dots, N\}$ είναι γνήσια.

Θα δώσουμε μια περιγραφή της απόδειξης του Θεωρήματος 5.3.1 στην τυπική περίπτωση όπου $G = \mathbb{F}_3^n$. Η απόδειξη ακολουθεί την ίδια γραμμή με αυτήν των Bateman και Katz, έχει όμως αρκετές ουσιώδεις διαφορές. Αυτές οι διαφορές δεν φαίνονται αρκετά στην περίπτωση $G = \mathbb{F}_3^n$, είναι όμως κρίσιμες για τον σκοπό μας όταν $G = \mathbb{Z}_N$.

5.3.1 Αύξηση πυκνότητας

Έστω $A \subset \mathbb{F}_3^n$ ένα σύνολο με πυκνότητα $\alpha = |A|/3^n$. Στόχος μας είναι να δώσουμε κάτω φράγμα για την ποσότητα $T(A)$. Η προσέγγιση που χρησιμοποιούμε είναι, όπως και στο αρχικό επιχείρημα του Roth, μέσω της αύξησης πυκνότητας. Αν το πλήθος των αριθμητικών προόδων μήκους 3 διαφέρει σημαντικά από αυτό που αναμένουμε σε ένα τυχαίο σύνολο με αυτή την πυκνότητα, τότε πρέπει να υπάρχει κάποιος υπόχωρος $V \leqslant \mathbb{F}_3^n$ μικρής συνδιάστασης στον οποίο κάποια μεταφορά του A έχει μεγαλύτερη πυκνότητα: $|(A+x)\cap V|/|V| \geqslant (1+\delta)\alpha$ για κάποιον $\delta > 0$. Παρατηρώντας ότι ένα κάττω φράγμα για το πλήθος των αριθμητικών προόδων μήκους 3 στο $(A+x)\cap V$ δίνει το ίδιο κάτω φράγμα για το πλήθος των αριθμητικών προόδων στο A, επαναλαμβάνουμε το ίδιο επιχείρημα, χρησιμοποιώντας τον V στη θέση του $\mathbb{F}_3^n$. Αφού η πυκνότητα δεν μπορεί ποτέ να γίνει μεγαλύτερη από 1, αυτό το επιχείρημα πρέπει να σταματήσει σε $\tilde{O}_\alpha(\delta^{-1})$ το πλήθος βήματα, και αν ο τελευταίος υπόχωρος εξακολουθεί να έχει αρκετά μεγάλη διάσταση, μπορούμε να δώσουμε ένα καλό κάτω φράγμα για την $T(A')$, όπου A' είναι κάποιο υποσύνολο μιας μεταφοράς του A, άρα και για την $T(A)$.

Περιγράφουμε αυτή την ιδέα με περισσότερες λεπτομέρειες. Έστω $V \leqslant \mathbb{F}_3^n$ και έστω A ένα υποσύνολο του V με πυκνότητα α. Λέμε ότι το A έχει αύξηση πυκνότητας με ισχύ $[d,\delta]$ ως προς τον V αν υπάρχει κάποιος $V' \leqslant V$ με συνδιάσταση το πολύ Cd τέτοιος ώστε

$$\|\mathbf{1}_A * \mu_{V'}\|_\infty = \sup_x \frac{|(A+x)\cap V'|}{|V'|} \geqslant (1+C^{-1}\delta)\alpha,$$

όπου $C = \tilde{O}_\alpha(1)$. Είναι σημαντικό να παρατηρήσουμε ότι, παρά την χρήση του γράμματος δ, η αύξηση πυκνότητας μπορεί να γίνει αρκετά μεγαλύτερη από 1 και σε κάποιες περιπτώσεις αρκετά μικρότερη.

Έστω $K = K(\alpha) \geqslant 1$ μια φθίνουσα συνάρτηση του α την οποία θα επιλέξουμε αργότερα, και η οποία θα παραμείνει σταθερή στην διάρκεια της απόδειξης. Θα δείξουμε ότι αν $V \leqslant \mathbb{F}_3^n$ και το $A \subset V$ έχει πυκνότητα α τότε πρέπει να ισχύει κάποιο από τα παρακάτω:

(i) (πολλές πρόοδοι) $T(A) \gg \alpha^3\mu(V)^2$, ή

(ii) το A έχει αύξηση πυκνότητας ως προς V με ισχύ (α) $[K^{-O(1)}, K^{O(1)}]$ (μικρή αύξηση) ή (β) $[K, K^{-1}\alpha^{-1}]$ (μεγάλη αύξηση).

Εκτός από αυτό το αποτέλεσμα αύξησης πυκνότητας, θα χρειαστούμε επίσης ένα ασθενέστερο κάτω φράγμα για την $T(A)$, το οποίο θα χρησιμοποιούμε συνεχώς: αν το $A \subset V \leqslant \mathbb{F}_3^n$ έχει σχετική πυκνότητα α τότε

$$T(A) \gg \exp(-O(\alpha^{-1}))\mu(V)^2. \tag{5.3.1}$$

Αυτό το φράγμα αποδεικνύεται εύκολα με μεθόδους ανάλυσης Fourier.

Εξηγούμε τώρα πώς μπορούμε να πάρουμε το φράγμα του Θεωρήματος 5.3.1 αν έχουμε στη διάθεσή μας αυτή τη διχοτομία για την αύξηση πυκνότητας. Ξεκινάμε με ένα υποσύνολο A του $V = \mathbb{F}_3^n$ που έχει πυκνότητα α, και εφαρμόζουμε διαδοχικά αυτή τη διχοτομία, αντικαθιστώντας κάθε φορά το A με κατάλληλο υποσύνολο μιας μεταφοράς και το V με κατάλληλο υπόχωρο. Αφού μια μικρή αύξηση μπορεί να συμβεί το πολύ $\tilde{O}_\alpha(K^{O(1)})$ φορές, και κάθε φορά η συνδιάσταση αυξάνεται κατά $\tilde{O}_\alpha(K^{O(1)})$, πρέπει τελικά να φτάσουμε σε κάποιον υπόχωρο V' με συνδιάσταση $\tilde{O}_\alpha(K^{O(1)})$ και κάποιο $A' \subset V'$ με σχετική πυκνότητα τουλάχιστον α, το οποίο είναι υποσύνολο μιας μεταφοράς του A, τέτοιο ώστε είτε να βρισκόμαστε στην πρώτη περίπτωση και να έχουμε $T(A') \gg \alpha^3\mu(V')^2$, ή αλλιώς να έχουμε κάποια μεγάλη αύξηση και άρα κάποιον $V'' \leqslant V'$ με συνδιάσταση $\tilde{O}(K^{O(1)} + K^{-1}\alpha^{-1})$ και κάποιο $A'' \subset V''$, το οποίο είναι υποσύνολο μιας μεταφοράς του A, με σχετική πυκνότητα $\gg_\alpha K\alpha$. Στην τελευταία περίπτωση, χρησιμοποιώντας το ασθενές φράγμα (5.3.1) παίρνουμε

$$T(A) \geqslant T(A'') \gg \exp(-\tilde{O}_\alpha(K^{-1}\alpha^{-1}))\mu(V'')^2.$$

Σε κάθε περίπτωση έχουμε

$$T(A) \gg \exp(-\tilde{O}_\alpha(K^{O(1)} + K^{-1}\alpha^{-1})).$$

Επιλέγοντας $K = \alpha^{-c'}$ για κάποια αρκετά μικρή σταθερά $c' > 0$ συμπεραίνουμε ότι

$$T(A) \geqslant \exp(-O(\alpha^{-1+c}))$$

όπως θέλαμε. Στο υπόλοιπο αυτής της περιγραφής εξηγούμε πώς προκύπτουν τα παραπάνω αποτελέσματα αύξησης πυκνότητας. Για απλότητα υποθέτουμε ότι $V = \mathbb{F}_3^n$.

5.3.2 Αριθμητικές πρόοδοι και μεγάλα φάσματα

Όπως και στην αρχική απόδειξη του Roth, εκφράζουμε την $T(A)$ χρησιμοποιώντας ανάλυση Fourier και παίρνουμε πληροφορίες για την $\widehat{\mathbf{1}_A}$. Ξεκινάμε από την ταυτότητα

$$T(A) = \sum_\gamma \widehat{\mathbf{1}_A}(\gamma)^3 = \alpha^3 + \sum_{\gamma \neq 0} \widehat{\mathbf{1}_A}(\gamma)^3$$

η οποία ισχύει μόνο όταν $G = \mathbb{F}_3^n$, όμως ανάλογη ταυτότητα ισχύει για οποιαδήποτε πεπερασμένη αβελιανή ομάδα. Ειδικότερα, αν για παράδειγμα $T(A) \leqslant \alpha^3/2$ τότε έχουμε

$$\sum_{\gamma \neq 0} |\widehat{\mathbf{1}_A}(\gamma)|^3 \gg \alpha^3.$$

Από την ταυτότητα Parseval έχουμε επίσης

$$\sum_\gamma |\widehat{\mathbf{1}_A}(\gamma)|^2 = \alpha.$$

Από αυτές τις δύο σχέσεις συμπεραίνουμε ότι υπάρχει κάποιο $\gamma \neq 0$ τέτοιο ώστε $|\widehat{\mathbf{1}_A}(\gamma)| \gg \alpha^2$. Η πληροφορία αυτή είναι ήδη μη τετριμμένη και από αυτήν μπορούμε να συμπεράνουμε ότι το A έχει αύξηση πυκνότητας μεγέθους $[\alpha, 1]$, κάτι που μπορεί να μας δώσει το κάτω φράγμα

$$T(A) \gg \exp(-O(\alpha^{-1})).$$

Εφαρμόζοντας όμως την δυαδική αρχή του περιστερώνα μπορούμε να αποδείξουμε κάτι ι-σχυρότερο. Ορίζουμε το φάσμα η-επιπέδου του A να είναι το

$$\Delta_\eta(A) = \{\gamma : |\widehat{\mathbf{1}_A}(\gamma)| \geqslant \eta\alpha\}.$$

Από την δυαδική αρχή του περιστερώνα, για κάποιον $1 \geqslant \eta \gg \alpha$ έχουμε

$$\sum_{\gamma \in \Delta_\eta(A) \setminus \Delta_{2\eta}(A), \gamma \neq 0} |\widehat{\mathbf{1}_A}(\gamma)|^3 \gg_\alpha \alpha^3,$$

άρα

$$|\Delta_\eta(A) \setminus \{0\}| \gg_\alpha \eta^{-3}.$$

Είναι καλό να συγκρίνουμε αυτό το φράγμα με το τετριμμένο άνω φράγμα $|\Delta_\eta(A)| \leqslant \eta^{-2}\alpha^{-1}$ που προκύπτει από την ταυτότητα Parseval. Θα πάρουμε την αύξηση πυκνότητας που θέλουμε βρίσκοντας μεγάλα υποσύνολα του φάσματος με σχετικά μικρή διάσταση (όπου διάσταση είναι ο πληθάριθμος του μικρότερου υποσυνόλου που παράγει το σύνολο). Ο καλύτερος τρόπος για να το κατταλάβουμε αυτό είναι με το συνηθισμένο L^2 επιχείρημα αύξησης το οποίο δείχνει ότι αν υπάρχει κάποιο $\Delta \subset \Delta_\eta(A) \setminus \{0\}$ με $|\Delta| \geqslant \delta\eta^{-2}$ και $\dim\Delta \leqslant d$ τότε το A έχει αύξηση πυκνότητας ισχύος $[\delta, d]$. Για να δούμε γιατί ισχύει αυτό, παρατηρούμε ότι αν

$$V = \{x \in \mathbb{F}_3^n : \gamma(x) = 1 \text{ για κάθε } \gamma \in \Delta\}$$

είναι ο υπόχωρος που μηδενίζει όλους τους χαρακτήρες στο Δ, τότε ο V έχει συνδιάσταση το πολύ d και

$$\begin{aligned}
\alpha\|\mathbf{1}_A * \mu_V\|_\infty &\geqslant \langle \mathbf{1}_A * \mu_V, \mathbf{1}_A * \mu_V \rangle \\
&= \langle \mathbf{1}_A \circ \mathbf{1}_A, \mu_V \circ \mu_V \rangle \\
&\geqslant \sum_{\Delta \cup \{0\}} |\widehat{\mathbf{1}_A}(\gamma)|^2 \\
&\geqslant \alpha^2 + \eta^2\alpha^2|\Delta|,
\end{aligned}$$

χρησιμοποιώντας το γεγονός ότι $|\widehat{\mu_V}|^2 \geqslant \mathbf{1}_{\Delta \cup \{0\}}$.

Με τη συζήτηση που έχουμε κάνει ως τώρα, μπορούμε να δείξουμε ότι είτε $T(A) \gg \alpha^3$ ή το A έχει αύξηση πυκνότητας με ισχύ $[1, \alpha^{-3}]$, κάτι που μας δίνει μόνο το φράγμα $T(A) \geqslant \exp(-\tilde{O}_\alpha(\alpha^{-1/3}))$. Για να το βελτιώσουμε, χρειαζόμαστε περισσότερες πληροφορίες και όχι μόνο το μέγεθος του φάσματος.

5.3.3 Προσθετική δομή του φάσματος

Σταθεροποιούμε τώρα κάποιο η τέτοιο ώστε $|\Delta_\eta(A)| \gg_\alpha \eta^{-3}$. Στόχος μας είναι να βρούμε μεγάλο υποσύνολο $\Delta \subset \Delta_\eta(A)$ με μικρή διάσταση.

Ένα βασικό αποτέλεσμα της Chang ισχυρίζεται ότι το ίδιο το $\Delta_\eta(A)$ έχει διάσταση $\tilde{O}_\alpha(\eta^{-2})$. Αυτό ήδη οδηγεί σε μια βελτίωση των παραπάνω, δίνοντας μια αύξηση πυκνότητας με ισχύ $[1, \alpha^{-2}]$, άρα $T(A) \geqslant \exp(-\tilde{O}_\alpha(\alpha^{-1/2}))$. Αυτό το αποτέλεσμα της Chang έχει παίξει σημαντικό ρόλο σε πολλές προηγούμενες προσεγγίσεις στο θεώρημα του Roth, και ήταν το πρώτο αποτέλεσμα που έξασφάλιζε μη τετριμμένη προσθετική δομή στα φάσματα. Αν και δεν θα το χρειαστούμε, παρόμοιες ιδέες χρησιμοποιούνται σε ό,τι ακολουθεί.

Η μέθοδος που θα χρησιμοποιήσουμε για να μελετήσουμε την προσθετική δομή των φασμάτων βασίζεται στις προσθετικές ενέργειες υψηλότερης τάξης. Για $m \geqslant 1$ ορίζουμε

$$E_{2m}(\Delta) = |\{\gamma_1 + \cdots + \gamma_m = \gamma_1' + \cdots + \gamma_m' : \gamma_i, \gamma_i' \in \Delta\}| = \mathbb{E}_x |\check{\mathbf{1}}_\Delta(x)|^{2m}.$$

Η ποσότητα αυτή βρίσκεται ανάμεσα στους $|\Delta|^m$ και $|\Delta|^{2m-1}$. Αν $\Delta \subset \Delta_\eta(A)$ τότε έχουμε το πολύ χρήσιμο κάτω φράγμα

$$E_{2m}(\Delta) \geqslant \alpha \eta^{2m} |\Delta|^{2m}$$

το οποίο προκύπτει από την ανισότητα $\langle |\widehat{\mathbf{1}_A}|, \mathbf{1}_\Delta \rangle \geqslant \eta\alpha|\Delta|$ με απλή εφαρμογή της ανισότητας Hölder. Η ανισότητα αυτή οφείλεται στον Shkredov, ο οποίος την χρησιμοποίησε για να δώσει μια εναλλακτική απόδειξη του αποτελέσματος της Chang.

Για να εκμεταλλευτούμε αυτό το κάτω φράγμα, θα χρησιμοποιήσουμε την παρατήρηση ότι ένα σύνολο με μεγάλη προσθετική ενέργεια υψηλής τάξης περιέχει μεγάλο υποσύνολο με μικρή διάσταση. Αυτό αποδεικνύεται με την πιθανοθεωρητική μέθοδο. Η τεχνική αυτή οφείλεται στους Bateman και Katz, οι οποίοι απέδειξαν ότι αν $E_{2m}(\Delta) \geqslant d^{-2m}|\Delta|^{2m}$ τότε το Δ έχει υποσύνολο Δ' με πληθάριθμο $|\Delta'| \gg m^{-O(1)}|\Delta|/d$ και διάσταση $\dim\Delta' \ll m^{O(1)}d$. Ειδικότερα, αν επιλέξουμε $m = C\lceil \log(2/\alpha) \rceil$ για κάποια μεγάλη σταθερά C και $d \approx \eta^{-1}$ τότε το μεγάλο φάσμα $\Delta_\eta(A)$ ικανοποιεί το κάτω φράγμα που ζητάμε για την ενέργεια, άρα έχουμε κάποιο $\Delta \subset \Delta_\eta(A)$ με πληθάριθμο $|\Delta| \gg_\alpha \eta^{-2}$ και διάσταση $\dim\Delta \ll_\alpha \eta^{-1}$. Έτσι παίρνουμε αύξηση πυκνότητας με ισχύ $[1, \eta^{-1}]$, που στη χειρότερη περίπτωση είναι ισχύς $[1, \alpha^{-1}]$, άρα μας δίνει το κάτω φράγμα $T(A) \gg \exp(-\tilde{O}_\alpha(\alpha^{-1}))$.

Στόχος μας είναι να πετύχουμε αύξηση πυκνότητας που έχει ισχύ $[K^{-O(1)}, K^{O(1)}]$ ή $[K, K^{-1}\alpha^{-1}]$, όπου K είναι δοσμένη παράμετρος, από το γεγονός ότι $|\Delta_\eta(A)| \gg_\alpha \eta^{-3}$ για κάποιον $1 \geqslant \eta \gg \alpha$.

Πρώτα χρησιμοποιούμε το παραπάνω πιθανοθεωρητικό επιχείρημα για να βρούμε κάποιο $\Delta_1 \subset \Delta_\eta(A)$ με πληθάριθμο $\approx \eta^{-2}$ και διάσταση $\ll_\alpha \eta^{-1}$. Στη συνέχεια αφαιρούμε αυτό το Δ_1 από το $\Delta_\eta(A)$ και αν παραμένει τουλάχιστον το μισό από το $\Delta_\eta(A)$ εφαρμόζουμε το επιχείρημα και πάλι. Επαναλαμβάνοντας αυτό το βήμα $\approx K$ φορές, παίρνοντας την ένωση όλων των κομματιών, και χρησιμοποιώντας το τετριμμένο άνω φράγμα $\dim(\Delta_1 \cup \cdots \cup \Delta_K) \leqslant \sum \dim(\Delta_i)$ για την διάσταση, παίρνουμε ένα σύνολο $\Delta \subset \Delta_\eta(A)$ με πληθάριθμο $|\Delta| \gg K\eta^{-2}$ και διάσταση $\dim\Delta \ll K\eta^{-1}$. Αυτή η διαδικασία μπορεί να ολοκληρωθεί αν $K^{-1} \gg_\alpha$

η. Αν επιπλέον υποθέσουμε ότι $\eta \gg K^2\alpha$ τότε παίρνουμε τι φράγμα $\ll_\alpha K^{-1}\alpha^{-1}$ για τη διάσταση, και η L^2 μέθοδος που έχουμε συζητήσει παραπάνω μας δίνει αύξηση πυκνότητας με ισχύ $[K, K^{-1}\alpha^{-1}]$, δηλαδή έχουμε πετύχει αύξηση πυκνότητας τόσο μεγάλη όσο θέλαμε.

Η περίπτωση $1 \geqslant \eta \gg_\alpha K^{-1}$ είναι ακόμη απλούστερη, αφού αν πάρουμε έναν μόνο χαρακτήρα από το $\Delta_\eta(A) \setminus \{0\}$ παίρνουμε μια μικρή αύξηση πυκνότητας με ισχύ $[K^{-1}, 1]$. Η δυσκολότερη περίπτωση είναι όταν $K^2\alpha \gg \eta \gg \alpha$. Στο υπόλοιπο αυτής της περιγραφής υποθέτουμε λοιπόν ότι $\eta = \alpha$ και ότι έχουμε ένα φάσμα $\Delta_\alpha(A)$ με πληθάριθμο $|\Delta_\alpha(A)| \gg_\alpha \alpha^{-3}$.

5.3.4 Δομή των μη-εξομαλυντικών συνόλων

Η μόνη περίπτωση που απομένει είναι όταν έχουμε ένα μεγάλο φάσμα στο επίπεδο α. Για $\Delta = \Delta_\alpha(A)$, τα φράγματα για την ενέργεια που συζητήσαμε πιο πάνω δείχνουν ότι $E_4(\Delta) \geqslant \alpha^5|\Delta|^4 \gg_\alpha \alpha^2|\Delta|^3$. Επιπλέον, μπορούμε να υποθέσουμε ότι το κάτω φράγμα $\alpha^9|\Delta|^8$ για την $E_8(\Delta)$ είναι περίπου ακριβές. Πράγματι, αν $E_8(\Delta) \geqslant K^6\alpha^9|\Delta|^8$ τότε μπορούμε να εφαρμόσουμε την ανισότητα Hölder και να βρούμε κάποιον μεγάλο $m \approx \log(2/\alpha)$ τέτοιον ώστε $E_{2m}(\Delta) \gg (mK\alpha)^{2m}|\Delta|^{2m}$, άρα υπάρχει $\Delta' \subset \Delta$ με πληθάριθμο $\gg_\alpha K\alpha^{-2}$ και διάσταση $\ll_\alpha K^{-1}\alpha^{-1}$ με την μέθοδο της προηγούμενης υποενότητας, οπότε έχουμε αύξηση πυκνότητας με ισχύ $[K, K^{-1}\alpha^{-1}]$.

Συμπεραίνουμε λοιπόν ότι το Δ ικανοποιεί τις

$$E_4(\Delta) \approx \alpha^2|\Delta|^3 \quad \text{και} \quad E_8(\Delta) \approx \alpha^6|\Delta|^7,$$

αγνοώντας σφάλματα $K^{O(1)}$ τα οποία είναι πολυωνυμικά ως προς K. Αν θεωρήσουμε τις κανονικοποιημένες ενέργειες $e_4(\Delta) = E_4(\Delta)/|\Delta|^3$ και $e_8(\Delta) = E_8(\Delta)/|\Delta|^7$, τότε η προηγούμενη σχέση παίρνει τη μορφή $e_8 \approx e_4^3$. Με απλή εφαρμογή της ανισότητας Hölder βλέπουμε ότι $e_8 \geqslant e_4^3$ για κάθε σύνολο, άρα η E_8-ενέργεια του Δ είναι πολύ μικρή, η μικρότερη που θα μπορούσε να είναι για δοθείσα $E_4(\Delta)$. Η ιδέα, που προέρχεται από τους Bateman και Katz, είναι ότι μπορούμε να εκμεταλλευτούμε αυτή την πληροφορία για να πάρουμε δομική πληροφορία για το Δ.

Οι Bateman και Katz ονομάζουν τα σύνολα Δ με την ιδιότητα $e_8 \approx e_4^3$ προσθετικά μη-εξομαλυντικά σύνολα, και αποδεικνύουν ένα θεώρημα δομής για τέτοια σύνολα σε κάποιες περιπτώσεις. Χοντρικά, αν το Δ είναι μη-εξομαλυντικό τότε είτε (α) $\Delta \approx H \oplus X$, όπου $|X| \approx \alpha^{-2}$, $|H| \approx \alpha^{-1}$ και $\dim H \ll 1$, είτε (β) $\Delta \approx \bigsqcup_{i=1}^{L} H_i$, όπου $|H_i| \approx \alpha^{-2}$, $L \approx \alpha^{-1}$ και $\dim H_i \ll 1$.

Μία τέτοια δομική ανάλυση αποδείχθηκε από τους Bateman και Katz. Όταν $G = \mathbb{F}_3^n$, όπως στην περίπτωση που συζητάμε εδώ, μπορούμε να χρησιμοποιήσουμε αυτήν την ανάλυση, όταν όμως $G = \mathbb{Z}_N$ χρειαζόμαστε ένα πιο εκλεπτυσμένο δομικό αποτέλεσμα το οποίο θα συζητήσουμε παρακάτω.

Στη δεύτερη περίπτωση, έχουμε αμέσως ένα σύνολο $\Delta' \subset \Delta_\alpha(A)$ με πληθάριθμο $|\Delta'| \approx \alpha^{-2}$ και διάσταση $\dim\Delta' \ll 1$, οπότε παίρνουμε μια αύξηση πυκνότητας ισχύος $[1,1]$. Η δύσκολη περίπτωση είναι η πρώτη, στην οποία η απλοϊκή εφαρμογή της L^2 μεθόδου αύξησης δίνει είτε αύξηση ισχύος $[\alpha, 1]$ (αν απλώς θεωρήσουμε $H \subset \Delta$) ή ισχύος $[1, \alpha^{-1}]$ (αν θεωρήσουμε $H \oplus X' \subset \Delta$ όπου $|X'| \approx \alpha^{-1}$), και καμία από τις δύο δεν είναι αρκετά ισχυρή για το σκοπό μας.

5.3.5 Φασματική ενίσχυση

Η τελευταία και δυσκολότερη περίπτωση είναι όταν το $\Delta_\alpha(A)$ έχει τη μορφή $\Delta_\alpha(A) \approx H \oplus X$, όπου $|H| \approx \alpha^{-1}$, $|X| \approx \alpha^{-2}$, και το H έχει διάσταση $\tilde{O}_\alpha(1)$. Σε αυτή την περίπτωση, οι Bateman και Katz βρίσκουν έναν χαρακτήρα γ τέτοιον ώστε $|\widehat{\mathbf{1}_A}(\gamma)| \gg K\alpha^2$, το οποίο δίνει αύξηση πυκνότητας ισχύος $[K\alpha, 1]$. Όταν $G = \mathbb{F}_3^n$ αυτό είναι αρκετό για να αποδείξουμε το αποτέλεσμα που ζητάμε. Στην περίπτωση όμως των ακεραίων, επειδή πρέπει να δουλέψουμε με προσεγγιστικές και όχι ακριβείς υποομάδες, αυτή η αύξηση είναι πολύ ασθενής. Αυτό συμβαίνει διότι κάθε φορά που επαναλαμβάνουμε το επιχείρημα προκύπτει κάποιο κόστος το οποίο οφείλεται στο γεγονός ότι οι υποομάδες είναι μόνο προσεγγιστικές. Αυτά τα κόστη προστίθενται γρήγορα, οπότε θα θέλαμε μια αύξηση ισχύος $[\delta, d]$ με μεγαλύτερη τιμή του δ, ώστε να χρειαστούμε λιγότερα βήματα, ακόμη κι αν γι' αυτό χρειαστεί να μεγαλώσουμε το d. Χοντρικά, μια αύξηση πυκνότητας ισχύος $[\delta, d]$ δίνει το φράγμα $T(A) \gg \exp(-\tilde{O}_\alpha(\delta^{-1}d))$ στον $\mathbb{F}_3^n$ αλλά μόνο $T(A) \gg \exp(-\tilde{O}_\alpha(\delta^{-2}d))$ στο $\mathbb{Z}_N$.

Αυτό σημαίνει ότι χρειάζεται να δημιουργήσουμε αύξηση ισχύος $[K\alpha, 1]$ από έναν μόνο μεγάλο συντελεστή Fourier, αλλά αύξηση ισχύος $[1,1]$ από μια μεγάλη συλλογή συντελεστών Fourier με μικρή διάσταση, το οποίο αν θυμηθούμε ότι προκύπτουν σφάλματα πολυωνυμικά ως προς K, δίνει τελικά ισχύ $[K^{-O(1)}, K^{O(1)}]$.

Απαιτείται λοιπόν μια νέα τεχνική, την οποία ονομάζουμε φασματική ενίσχυση. Η φιλοσοφία αυτής της τεχνικής είναι ότι, ακριβώς όπως τα υποσύνολα των φασμάτων είναι προσθετικά δομημένα, ένα υποσύνολο ενός φάσματος το οποίο έχει ασυνήθιστα μεγάλη προσθετική δομή είναι υποχρεωμένο να έχει κάποια μεταφορά που βρίσκεται σε ένα φάσμα υψηλότερου επιπέδου. Δηλαδή, το «φασματικό επίπεδο» ενός συνόλου «ενισχύεται» αυτομάτως από την εγγενή προσθετική δομή του.

Για να δούμε γιατί αυτό είναι χρήσιμο, παρατηρούμε ότι κάποια μεταφορά του H βρίσκεται στο $\Delta_\alpha(A)$, και $|H| \approx \alpha^{-1}$. Αφού $\dim H \ll_\alpha 1$, εφαρμόζοντας την L^2 μέθοδο αύξησης πυκνότητας απλοϊκά παράγουμε αύξηση πυκνότητας με ισχύ $[\alpha^2|H|, 1] = [\alpha, 1]$ χρησιμοποιώντας μόνο το γεγονός ότι το H είναι υποσύνολο του $\Delta_\alpha(A)$. Η φασματική ενίσχυση μας επιτρέπει να εκμεταλλευτούμε το γεγονός ότι το H έχει πλούσια προσθετική δομή για να βρούμε μια μεταφορά του H που συμπεριφέρεται σαν υποσύνολο του $\Delta_{\alpha^{1/2}}(A)$. Αυτό σημαίνει ότι η L^2 μέθοδος μας δίνει τώρα μια πολύ ισχυρή αύξηση πυκνότητας με ισχύ $[\alpha|H|,1]=[1,1]$ όπως θέλαμε. Τονίζουμε εδώ ότι οι υποθέσεις που πρέπει να ικανοποιούνται για να δουλέψει η φασματική ενίσχυση είναι πολύ αυστηρές, όμως, ευτυχώς, στην περίπτωσή μας αν αυτές δεν ισχύουν τότε μπορούμε να χρησιμοποιήσουμε εναλλακτικά τις μεθόδους που έχουμε ήδη συζητήσει.

Μένει να περιγράψουμε τον τρόπο με τον οποίο δουλεύει η φασματική ενίσχυση. Ας υποθέσουμε ότι το $\Delta=\Delta_\alpha(A)$ έχει σχεδόν μέγιστο πληθάριθμο $|\Delta|\approx\alpha^{-3}$ και ότι υπάρχει κάποιο σύνολο $H\subset\Delta$ τέτοιο ώστε

$$|H|\approx\alpha^{-1}\quad\text{και}\quad\langle\mathbf{1}_\Delta\circ\mathbf{1}_\Delta,\mathbf{1}_H\circ\mathbf{1}_H\rangle\approx|\Delta|\,|H|^2.$$

Αυτός είναι ο τύπος προσθετικής δομής που ζητάμε για το H, και είναι εύκολο να ελέγξουμε ότι υπάρχει αν $\Delta\approx H\oplus X$ όπως παραπάνω. Η ιδέα είναι να συνδυάσουμε αυτήν την προσθετική πληροφορία με το γεγονός ότι $\Delta=\Delta_\alpha(A)$ εφαρμόζοντας την ανισότητα Cauchy-Schwarz και δουλεύοντας τόσο στον φυσικό χώρο όσο και στον χώρο των συχνοτήτων.

Το πρώτο βήμα είναι να χρησιμοποιήσουμε την φασματική πληροφορία $\mathbf{1}_\Delta\ll\alpha^{-4}|\widehat{\mathbf{1}_A}|^2$ για να πάρουμε το φράγμα

$$\left\langle|\widehat{\mathbf{1}_A}|^2*\mathbf{1}_H\circ\mathbf{1}_H,\mathbf{1}_\Delta\right\rangle\gg\alpha^4|\Delta|\,|H|^2.$$

Αν προσπαθήσουμε να φράξουμε αυτό το εσωτερικό γινόμενο χρησιμοποιώντας τετριμμένα την L^1 και την L^∞ νόρμα, παίρνουμε απλώς το φράγμα

$$\|\,|\widehat{\mathbf{1}_A}|^2*\mathbf{1}_H\|_\infty\gg\alpha^4|H|.$$

Δηλαδή, υπάρχει κάποια μεταφορά του H στην οποία η μέση τιμή της $|\widehat{\mathbf{1}_A}|$ είναι $\gg\alpha^2$, κάτι που ούτως ή άλλως γνωρίζουμε αφού το H είναι υποσύνολο του φάσματος α-επιπέδου. Θα δείξουμε τώρα ότι, υποθέτοντας κάποιες πρόσθετες φυσιολογικές συνθήκες, μπορούμε να δείξουμε ότι το H (ή κάποια μεταφορά του) συμπεριφέρεται σαν υποσύνολο του φάσματος $\alpha^{1/2}$-επιπέδου.

Πρώτα μεταφέρουμε την προηγούμενη ανισότητα στον φυσικό χώρο: έχουμε

$$\mathbb{E}_x\mathbf{1}_A\circ\mathbf{1}_A(x)|\check{\mathbf{1}}_H(x)|^2\sum_\gamma\mathbf{1}_\Delta(\gamma)\gamma(x)\gg\alpha^4|\Delta|\,|H|^2.$$

Εφαρμόζοντας την ανισότητα Cauchy-Schwarz και πηγαίνοντας πίσω στον χώρο των συχνοτήτων, έχουμε

$$\left\langle|\widehat{\mathbf{1}_A}|^2,\mathbf{1}_H\circ\mathbf{1}_H\right\rangle\left\langle|\widehat{\mathbf{1}_A}|^2*\mathbf{1}_H\circ\mathbf{1}_H,\mathbf{1}_\Delta\circ\mathbf{1}_\Delta\right\rangle\gg\alpha^8|\Delta|^2|H|^4.$$

Μπορούμε να φράξουμε το δεύτερο εσωτερικό γινόμενο χρησιμοποιώντας πρώτα την ανισότητα Cauchy-Schwarz, μετά περνώντας στον φυσικό χώρο, και χρησιμοποιώντας την τετριμμένη ανισότητα $|\check{\mathbf{1}}_H|\leqslant|H|$, οπότε παίρνουμε

$$\left\langle|\widehat{\mathbf{1}_A}|^2*\mathbf{1}_H\circ\mathbf{1}_H,\mathbf{1}_\Delta\circ\mathbf{1}_\Delta\right\rangle^2\leqslant\sum|\widehat{\mathbf{1}_A}|^4|H|^4E_4(\Delta).$$

Ας υποθέσουμε προς στιγμήν ότι μπορούμε να αγνοήσουμε τον τετριμμένο χαρακτήρα στο άθροισμα του δεξιού μέλους. Μπορούμε να υποθέσουμε ότι το μεγαλύτερο μέρος της «μάζας Fourier» του A (εκτός από τον τετριμμένο χαρακτήρα) είναι συγκεντρωμένο στο Δ (αλλιώς μπορούμε να πραγματοποιήσουμε ολόκληρο το επιχείρημα σε κάποιο φασματικό επίπεδο πολύ μεγαλύτερο από α, κάτι που έχουμε ήδη αντιμετωπίσει πιο πάνω). Έπεται ότι

$$\sum_{\gamma\neq 0} |\widehat{\mathbf{1}_A}(\gamma)|^4 \ll \alpha^8|\Delta|.$$

Επιπλέον, όπως παραπάνω, μπορούμε να υποθέσουμε ότι ισχύει άνω φράγμα της μορφής $E_4(\Delta) \ll \alpha^5|\Delta|^4$, αλλιώς μπορούμε να βρούμε μεγάλο υποσύνολο με μικρή διάσταση και έχουμε τελειώσει. Συνδυάζοντας αυτά τα φράγματα με τα παραπάνω, τώρα παίρνουμε

$$\big\| \, |\widehat{\mathbf{1}_A}|^2 * \mathbf{1}_H \, \big\|_\infty \gg \alpha^{3/2}|\Delta|^{-1/2}|H| \gg \alpha^3|H|.$$

Ειδικότερα, έχουμε κερδίσει έναν παράγοντα α σε σύγκριση με το προηγούμενο τετριμμένο φράγμα, δηλαδή κατά μέσο όρο έχουμε $|\widehat{\mathbf{1}_A}| \gg \alpha^{3/2}$ στο H, όπως θέλαμε.

Υπάρχει ένα ακόμη σοβαρό εμπόδιο για την εφαρμογή αυτής της στρατηγικής, που είναι η παρουσία του τετριμμένου χαρακτήρα, τον οποίο πρέπει να αφαιρέσουμε αλλιώς έχουμε $\sum |\widehat{\mathbf{1}_A}|^4 \geqslant \alpha^4$ κατά τετριμμένο τρόπο. Για το σκοπό αυτό αντικαθιστούμε στην αρχή την $\mathbf{1}_A$ από την ισορροπημένη συνάρτηση $f = \mathbf{1}_A - \alpha$ που έχει μηδενικό συντελεστή Fourier στον τετριμμένο χαρακτήρα. Επαναλαμβάνουμε ολόκληρη την απόδειξη που περιγράψαμε για την ισορροπημένη συνάρτηση, τώρα όμως αντιμετωπίζουμε το πρόβλημα ότι η πρώτη εφαρμογή της ανισότητας Cauchy-Schwarz πιο πάνω αντικαθιστά την $f \circ f$ με την $|f \circ f|$. Συνεπώς, τελικά αντιμετωπίζουμε το πρόβλημα του να μετατρέψουμε την απόκλιση για την απόλυτη τιμή της ισορροπημένης συνάρτησης του A σε μια γνήσια αύξηση πυκνότητας για το A. Αυτό επιτυγχάνεται με τις τεχνικές σχεδόν περιοδικότητας των Croot και Sisask που μελετήσαμε στο Κεφάλαιο 3. Παίρνουμε έτσι μια αύξηση πυκνότητας με ισχύ $[1,1]$ (η οποία είναι μάλιστα $[K^{-O(1)}, K^{O(1)}]$ αφού έχουμε αγνοήσει πολυωνυμικά ως προς K σφάλματα) και έτσι ολοκληρώνουμε την απόδειξη.

Βιβλιογραφία

[1] M. Bateman and N. H. Katz, *New bounds on cap sets*, J. Amer. Math. Soc. 25 (2012), 585–613.

[2] T. F. Bloom, *A quantitative improvement for Roth's theorem on arithmetic progressions*, J. Lond. Math. Soc. (2) 93 (2016), 643–663.

[3] T. F. Bloom and O. Sisask, *Logarithmic bounds for Roth's theorem via almost-periodicity*, Discrete Anal. 2019, Paper No. 4, 20 pp.

[4] T. F. Bloom and O. Sisask, *Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions*, Preprint.

[5] J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. 9 (1999), 968–984.

[6] J. Bourgain, *Roth's theorem on progressions revisited*, J. Anal. Math. 104 (2008), 155–192.

[7] E. Croot, I. Laba and O. Sisask, *Arithmetic progressions in sumsets and L_p-almost-periodicity*, Combin. Probab. Comput. 22 (2013), 351–365.

[8] E. Croot and O. Sisask, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. 20 (2010), 1367–1396.

[9] D. R. Heath-Brown, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. 35 (1987), 385–394.

[10] M. G. Kendall, *The advanced theory of statistics*, volume 1, second edition, 1945.

[11] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. 28 (1953), 104–109.

[12] T. Sanders, *On Roth's theorem on progressions*, Ann. of Math. 174 (2011), 619–636.

[13] T. Sanders, *On certain other sets of integers*, J. Anal. Math. 116 (2012), 53–82.

[14] T. Sanders, *Additive structures in sumsets*, Math. Proc. Cambridge Philos. Soc. 144 (2008), 289–316.

[15] T. Schoen and O. Sisask, *Roth's theorem for four variables and additive structures in sums of sparse sets*, Forum Math. Sigma 4 (2016), e5.

[16] E. Szemerédi, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. 56 (1990), 155–158.

[17] T. Tao and V. Vu, *Additive Combinatorics*, 1st ed. Cambridge University Press, 2006.