ΑΚΡΙΒΗΣ ΑΝΑΚΤΗΣΗ ΣΗΜΑΤΟΣ ΑΠΟ ΕΛΛΙΠΕΙΣ ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟΥΣ ΣΥΝΤΕΛΕΣΤΕΣ **FOURIER** ΤΟΥ ΣΗΜΑΤΟΣ

Ευτύχης Φραγκιουδάκης
Τμήμα Μαθηματικών
Πανεπιστήμιο Κρήτης
Επιβλέπων Καθηγητής: Κολουντζάκης Μιχαήλ

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Περίληψη.

Το βασικό θέμα αυτής της εργασίας είναι το πρόβλημα ανάκτησης ενός σήματος από ελλειπή γνώση για τις συχνότητες του σήματος. Θα εξετάσουμε ποιες είναι οι προυποθέσεις ώστε να ανακτήσουμε ένα σήμα από μερική γνώση των συντελεστων Fourier του σήματος. Πρώτα θα εξετάσουμε την περίπτωση όπου το μήκος του σήματος είναι πρώτος αριθμος και θα δούμε πότε μπορούμε να έχουμε ακριβή ανάκτηση. Στην περίπτωση που το μήκος δεν είναι πρώτος θα προσεγγίσουμε το πρόβλημα πιθανοθεωριτικά όπου θα αναπτύξουμε το μοντέλο που θα δουλέψουμε και θα δούμε τι πρέπει να ισχύει για να έχουμε ανάκτηση του σήματος με μεγάλη πιθανότητα. Η εργασία βασίζεται σε δύο paper των Terence Tao, Emmanuel Candes και Justin Romberg.

Το πρώτο κεφάλαιο της εργασίας αναφέρεται στην περίπτωση που το μήκος του σήματος είναι πρώτος αριθμός. Θα δούμε την (μια) αρχή αβεβαιότητας για κυκλικές ομάδες με τάξη πρώτο αριθμό, κάποιες εφαρμογές όπως η ανισότητα Cauchy Davenport και στην συνέχεια το θεώρημα για την ακριβή ανάκτηση ενός σήματος. Πιο αναλυτικά αν G μια πεπερασμένη ομάδα και f μια συνάρτηση τότε ο φορέας των f και $\hat{f}$ (εύκολα) θα δούμε ότι σχετίζονται ως εξής

$$|supp(f)||supp(\hat{f})| \geq |G|.$$

Αν τώρα η G είναι μια Z_p, με p πρώτο τότε θα δούμε ότι ο φορέας των f και $\hat{f}$ σχετίζονται ως εξής (αρχή της αβεβαιότητας)

$$|supp(f)| + |supp(\hat{f})| \geq p + 1.$$

Μια άμεση συνέπεια αυτής της αρχής της αβεβαιότητας είναι ότι αν έχω ένα πολυώνυμο $\sum_{j=0}^{k} c_j z^{n_j}$ με $k+1$ μη μηδενικούς συντελεστές και $0 \leq n_0 < ... < n_k < p$ τότε αν το περιοριστούμε στις p-οστές ρίζες της μονάδας, έχει το πολύ k ρίζες. Μια Δεύτερη είναι η ανισότητα Cauchy-Davenport που λέει ότι για κάθε δύο πεπερασμένα μη κενά υποσύνολα του $\mathbb{Z}_p$ έχουμε ότι για το σύνολο $A + B = \{a + b : a \in A, b \in B\}$ ότι

$$|A + B| \geq min(|A| + |B| - 1, p).$$

Τέλος θα δούμε ότι αν έχουμε ένα σήμα f μήκους P (P πρώτος αριθμός), $\Omega \subset Z_P$ όπου έχουμε γνώση για τους συντελεστές Fourier μόνο πάνω στο Ω και αν ο φορέας της f είναι το σύνολο T, τέτοιο ώστε

$$|T| \leq \frac{1}{2}|\Omega|$$

τότε μπορουμε να ανακτήσουμε πλήρως και με μοναδικό τρόπο την f από τα Ω και $\hat{f}|\Omega$.

Για την γενική περίπτωση (όταν το μήκος του σήματος δεν είναι κατ' ανάγκη πρώτος) θα δούμε ότι αν έχουμε ότι

$$|T| \leq C_M(\log N)^{-1}|\Omega|$$

όπου C_M είναι μια σταθερά, τότε με μεγάλη πιθανότητα, τουλάχιστον $1-O(N^{-M})$, μπορουμε να ανακτήσουμε πλήρως και με μοναδικό τρόπο την f ως λύση του παρακάτω προβλήματος βελτιστοποίησης: $min_{g \in C^N} ||g||_{l_1} := \sum_{t \in Z_N} |g(t)|$, τέτοιο ώστε $\hat{g}|_\Omega = \hat{f}|_\Omega$ για κάθε $\omega \in \Omega$. Το παραπάνω αποτελεί το βασικό μας θεώρημα και είναι το σημαντικότερο αποτέλεσμα της

εργασίας το οποίο ουσιαστικά μας λέει ότι όταν το ο φορεας T της f είναι της τάξης του Ω μόντουλο μια σταθερά και ένα λογαριθμικό παράγοντα τότε ουσιαστικά δεν χάνουμε πληροφορίες, δηλαδή μπορούμε να έχουμε ακριβή ανάκτηση της f.

Για να το δείξουμε αυτό θα δούμε ότι μια ικανή και αναγκαία συνθήκη για την f ώστε να είναι η λύση του προβλήματος βελτιστοποίησης είναι η ύπαρξη ενός τριγωνομετρικού πολυωνύμου P του οποίου ο φορέας του μετασχηματισμού Fourier είναι πάνω στο Ω, $P(t) = sgn(f)$ στο T και στο συμπλήρωμα του T είναι μικρότερο από την μονάδα. Αυτό το πολυώνυμο θα δούμε ότι είναι το εξής

$$P = F_{\Omega}^{*} F_{T\to\Omega} \left(F_{T\to\Omega}^{*} F_{T\to\Omega}\right)^{-1} i^{*} sgn(f)$$

και στην συνέχεια θα προσπαθήσουμε να αποδείξουμε τις ιδιότητες που έχει. Για να τις αποδείξουμε θα χρειαστούμε τον παρακάτω βοηθιτικό πίνακα

$$Hf(t) = -\sum_{\omega\in\Omega} \sum_{t'\in T: t'\neq t} e^{2\pi i \frac{\omega(t-t')}{N}} f(t')$$

καθώς επίσης και σειρές Neumann.

Το τελευταίο κεφάλαιο είναι η απόδειξη του θεωρήματος 3.3 το οποίο είναι μια εκτίμηση για την αναμενόμενη τιμή του ίχνους του βοηθιτικού πίνακα. Ειδικότερα, η εκτίμηση είναι η εξής

- $$E[Tr(H_0^{2n})] \leq 2\left(\frac{4}{e(1-\tau)}\right)^{n} n^{n+1} |\tau N|^{n} |T|^{n+1}$$
  όταν $n \leq \frac{\tau N}{4(a-\tau)|T|}$
- $$E[Tr(H_0^{2n})] \leq \frac{n}{1-\tau}(4n)^{2n-1} |\tau N||T|^{2n}$$
  διαφορετικά.

Για να την απόδειξη, που είναι αρκετά τεχνική, θα χρειαστεί να ορίσουμε σχέσεις ισοδυναμίας για να απλοποιήσουμε κάποια αθροισματα, να χρησιμοποιήσουμε από την συνδιαστική τους αριθμούς Stirling και τέλος να χρησιμοποιήσουμε την γνωστή προσέγγιση Stirling. Τα παραπάνω είναι πολύ τεχνικά και στα πλαίσια της περίληψης της εργασίας δεν είναι δυνατόν να δώσουμε παραπάνω πληροφορίες. Όποιος θέλει να δει τα παραπάνω μπορεί να ανατρέξει στο τελευταίο κεφάλαιο της εργασίας που είναι αναλυτικά γραμμένα.

ΚΕΦΑΛΑΙΟ 2

Η αρχή της αβεβαιότητας για κυκλικές ομάδες με τάξη πρώτο αριθμό.[1]

Εισαγωγή.

Σε αυτό το κεφάλαιο θα δείξουμε την σχέση που έχει ο φορέας μιας μιγαδικής συνάρτησης ορισμένη πάνω σε μια πεπερασμένη αβελιανή προσθετική ομάδα με τον φορέα του μετασχηματισμου Fourier της. Στην συνέχεια θα εξετάσουμε τι γίνεται στην ειδική περίπτωση που έχουμε την κυκλική ομάδα Z_p (όπου p πρώτος) και θα δώσουμε κάποιες εφαρμογές. Τέλος θα εξετάσουμε τις προυποθέσεις που χρειάζεται να πληρούνται ώστε να μπορούμε να ανακτήσουμε πλήρως ένα σήμα, όταν το μήκος του είναι πρώτος αριθμός, καθώς και ένα παράδειγμα όπου αποτυγχάνει αυτή η μέθοδος.

Έστω G μια πεπερασμένη αβελιανή, προσθετική ομάδα και $e : G\times G \to \{z \in \mathbb{C} : |Z| = 1\}$ μια συνάρτηση που οι τιμές της είναι πάνω στον μοναδιαίο κύκλο και ισχύει ότι

$$e(\chi + \chi', \xi) = e(\chi, \xi)e(\chi', \xi)$$
$$e(\chi, \xi + \xi') = e(\chi, \xi)e(\chi, \xi')$$

και για κάθε $\chi \neq 0$ υπάρχει $\xi \in G$ τέτοιο ώστε $e(\chi, \xi) \neq 1$, και όμοια για την δεύτερη μεταβλητή, για κάθε $\xi \neq 0$ υπάρχει $\chi \in G$ τέτοιο ώστε $e(\chi, \xi) \neq 1$.

Για παράδειγμα αν πάρουμε την ομάδα Z_N τότε εύκολα μπορούμε να δούμε ότι η $e(\chi, \xi) := e^{2\pi i\chi\xi/N}$ ικανοποιεί τις παραπάνω απαιτήσεις. Αν τώρα έχουμε $f : G \to \mathbb{C}$ μια μιγαδική συνάρτηση στο G, μπορούμε να ορίσουμε τον μετασχηματισμό Fourier της, $\hat{f} : G \to \mathbb{C}$ ως

$$\hat{f}(\xi) := \frac{1}{|G|}\sum_{x\in G} f(\chi)\overline{e(\chi, \xi)}$$

όπου $|G|$ είναι είναι η τάξη της πεπερασμένης ομάδας G. Παρατηρείστε ότι σε αυτήν την περίπτωση εξακολουθούν να ισχύουν οι βασικές ιδιότητες του μετασχηματισμού Fourier, όπως τις ξέρουμε από το $\mathbb{R}$.[2][3]

Αν $supp(f) = \{x \in G : f(x) \neq 0\}$ ο φορέας της f τότε χρησιμοποιώντας τον τύπο του μετασχηματισμου Fourier και την τριγωνική ανισότητα έχουμε ότι

$$\sup_{\xi\in G}|\hat{f}(\xi)| \leq \frac{1}{|G|}\sum_{\chi\in G}|f(\chi)| = \frac{1}{|G|}\sum_{\chi\in supp(f)}|f(\chi)| = \frac{(1, ..., 1)}{\sqrt{|G|}}\frac{(|f(\chi_1)|, ..., |f(\chi_{|G|})|)}{\sqrt{|G|}}$$

όπου τα διανύσματα έχουν $|supp(f)|$ συντεταγμενες. Στην συνέχεια από την ανισότητα Cauchy - Schwarz και το θεώρημα του Plancherel παίρνουμε ότι

$$\sup_{\xi}|\hat{f}(\xi)| \leq \frac{|supp(f)|^{1/2}}{|G|^{1/2}}\left(\frac{1}{|G|}\sum_{\chi\in supp(f)}|f(\chi)|^2\right)^{1/2} = \frac{|supp(f)|^{1/2}}{|G|^{1/2}}\left(\frac{1}{|G|}\sum_{\chi\in G}|f(\chi)|^2\right)^{1/2}$$
$$= \frac{|supp(f)|^{1/2}}{|G|^{1/2}}\left(\frac{1}{|G|}\sum_{\xi\in G}|\hat{f}(\xi)|^2\right)^{1/2}$$

και τελικά έχω ότι

$$\sup_{\xi} |\hat{f}(\xi)| \leq \frac{|supp(f)|^{1/2}||supp(\hat{f})|^{1/2}}{|G|^{1/2}} sup_{\xi \in G}|\hat{f}(\xi)|$$

αφού

$$\sum_{\xi \in G} |\hat{f}(\xi)|^2 \leq |supp(\hat{f})| sup_{\xi \in G}|\hat{f}(\xi)|^2.$$

Άρα όταν η f δεν είναι παντού μηδεν έχω ότι

$$|supp(f)||supp(\hat{f})| \geq |G| \tag{1}$$

Αξιζει να παρατηρήσουμε ότι αυτή η προσέγγιση δεν είναι χονδροειδής, καθώς αν η f (ή η $\hat{f}$) είναι η συνάρτηση του Dirac τότε έχουμε ισότητα.

Στην περίπτωση που η G είναι η Z_p για κάποιο πρώτο αριθμό p και $e(\chi, \xi) = e^{2\pi i \chi \xi / p}$, έχουμε ότι οι μόνες υποομάδες της G είναι οι τετριμμένες, δηλαδή, $\{0\}$ και G. Αυτό σημαίνει ότι η ανισότητα (1) είναι γνήσια, οπότε θα μπορούσαμε να την βελτιώσουμε. Το παρακάτω θεώρημα μας δίνει μια αισθητά καλύτερη εκτίμηση για τους φορείς των f και $\hat{f}$.

Θεώρημα 2.1. *Έστω p πρώτος. Αν $f : Z_p \to C$ είναι μια μη μηδενική, μιγαδική συνάρτηση τότε*

$$|supp(f)| + |supp(\hat{f})| \geq p + 1.$$

Αντίστροφα, αν A και B είναι δύο μη κενά υποσύνολα του Z_p τέτοια ώστε $|A| + |B| \geq p+1$ τότε υπάρχει μια συνάρτηση f τέτοια ώστε $supp(f) = A$ και $supp(\hat{f}) = B$.

Για να αποδείξουμε το θεώρημα θα χρειαστούμε κάποια λήμματα.

Λήμμα 2.2. *Έστω p ένας πρώτος αριθμός, n ένας θετικός ακέραιος και έστω $P(z_1, ..., z_n) \in \mathbb{Z}[z_1, ..., z_n]$ ένα πολυώνυμο με ακέραιους συντελεστές. Έστω ότι έχουμε n το πλήθος p-οστές ρίζες της μονάδας (όχι αναγκαστικά διαφορετικές), $\omega_1, ..., \omega_n$ τέτοιες ώστε $P(\omega_1, ..., \omega_n) = 0$. Τότε $P(1, ..., 1)$ είναι πολλαπλάσιο του p.*

Απόδειξη. Έχουμε $\omega_1, ..., \omega_n$ p-οστές ρίζες της μονάδας. Οπότε αν θέσουμε $\omega = e^{2\pi i/p}$ τότε για κάθε $1 \leq j \leq n$ θα έχουμε ότι $\omega_j = \omega^{k_j}$ για κάποιους ακέραιους με $0 \leq k_j < p$. Αν τώρα ορίσουμε το πολυώνυμο μιας μεταβλητής $Q(z) = P(z^{k_1}, ..., z^{k_n}) \bmod(z^p - 1)$ (άρα $deg(Q(z)) \leq p - 1$) έχουμε ότι $Q(\omega) = P(\omega^{z_1}, ..., \omega^{z_n}) = 0$ από υπόθεση και $Q(1) = P(1, ..., 1)$. Οπότε αρκεί να δείξω ότι το $Q(1)$ είναι πολαπλασιο του p. Αφού ω μια ρίζα του $Q(z)$, $deg(Q(z)) \leq p - 1$ και το $g(z) = 1 + z + z^1 + ... + z^{p-1}$ είναι το ελάχιστο μονικό $\mathbb{Q}$-πολυώνυμο που έχει ρίζα το ω θα έχουμε ότι $g(z)|Q(z)$. Άρα $Q(z) = g(z)h(z)$ για κάποιο h με συντελεστές εν γένει στο Q. Όμως αφού το Q πολυώνυμο ακέραιων συντελεστών και υπάρχουν πολυώνυμα g, h ρητών συντελεστων τέτοια ώστε $Q = gh$ τότε από το λήμμα του Gauss τα g, h είναι πολυώνυμα ακέραιων συντελεστων. Οπότε για $z = 1$ έχουμε ότι $Q(1) = g(1)h(1)$, με $g(1) = p$, άρα το $Q(1)$ είναι πολλαπλάσιο του p. □

Χρησιμοποιώντας το προηγούμενο Λήμμα, μπορούμε να αποδείξουμε ότι τα minors του πίνακα Fourier είναι μη μηδενικά.

Λήμμα 2.3. *Έστω p πρώτος και $1 \leq n \leq p$, $\chi_1, ..., \chi_n$ διαφορετικά στοιχεία του Z_p, $\xi_1, ..., \xi_n$ διαφορετικά στοιχεία επίσης του Z_p. Τότε η ορίζουσα του πίνακα $(e^{2\pi i \chi_j \xi_k / p})_{1 \leq j,k \leq n}$ είναι διαφορετική από το μηδέν.*

Απόδειξη. Αν θέσουμε $\omega_j = e^{2\pi i\chi_j/p}$, τότε κάθε ω_j είναι μια ρίζα της μονάδας και επειδή τα $\chi_1, ..., \chi_n$ είναι διαφορετικά μεταξύ τους και $1 \leq n \leq p$ θα έχουμε n διαφορετικές ρίζες της μονάδας. Οπότε αρκεί να δείξουμε ότι η ορίζουσα

$$det(\omega_j^{\xi_k})_{1\leq j,k\leq n}$$

είναι διάφορη του μηδέν. Για να το αποδείξουμε θα χρησιμοποιήσουμε το αντιθετο-αντίστροφο από το προηγούμενο Λήμμα. Έστω το πολυώνυμο

$$D(z_1, ..., z_n) = det(z_j^{\xi_k})_{1\leq j,k\leq k}.$$

Τα ξ_k είναι διαφορετικά στοιχεία του Z_p, οπότε, διαλέγοντας κατάλληλο αντιπρόσωπο για κάθε ξ_k, τα παίρνω να είναι στοιχεία του συνόλου

$$\{0, 1, ..., p-1\}.$$

Έχουμε ότι το πολυώνυμο είναι ακέραιων συντελεστών όμως $D(1, ..., 1) = 0$ καθώς παίρνουμε μια ορίζουσα με το στοιχείο 1 σε όλες τις θέσεις, οπότε η τιμή της ορίζουσας είναι μηδέν. Επιπροσθέτως, το D είναι μηδέν όταν $z_j = z_{j'}$ για οποιαδήποτε $1 \leq j < j' \leq n$ αφού η ορίζουσα θα έχει δύο γραμμές ίδιες και άρα η τιμή της είναι μηδέν. Οπότε, αφού τα $z_j - z_{j'}$ είναι ρίζες του D, παραγοντοποιώντας το D ως προς τα $z_j - z_{j'}$ θα έχουμε ότι

$$D(z_1, ..., z_n) = P(z_1, ..., z_n) \prod_{1\leq j<j'\leq n} (z_j - z_{j'})$$

όπου το P είναι το πολυώνυμο που προκύπτει από την διαίρεση του D με το γινόμενο των $z_j - z_{j'}$ παραγόντων. Πάλι, αφού το D είναι πολυώνυμο με ακέραιους συντελεστές και γράφεται σαν γινόμενο δυο πολυωνύμων (εν γένει, εμάς μας ενδιαφέρει το P) με συντελεστές στο Q από το λήμμα του Gauss το P είναι πολυώνυμο με ακέραιους συντελεστές. Το πλήθος των γραμμικών παραγόντων $(z_j - z_{j'})$ είναι ακριβώς $\frac{n(n-1)}{2}$ αφου για το z_1 υπάρχουν $n-1$ το πλήθος διαφορετικά z_j, για το z_2, $n-1$ και συνεχίζοντας έτσι, για το z_{n-1} ένα. Άρα είναι $1+2+...+(n-1) = \frac{n(n-1)}{2}$ παράγοντες. Θα δείξουμε ότι το $P(1, ..., 1)$ δεν είναι πολλαπλασιο του p και άρα από το προηγούμενο Λήμμα (θα εφαρμόσουμε το αντίθετο-αντίστροφο του λήμματος) το $P(\omega_1, ..., \omega_n)$ είναι διάφορο του μηδενός. Για να υπολογίσουμε το $P(1, ..., 1)$, θα παραγωγίσουμε το D. Πιο συγκεκριμένα θα εξετάσουμε την έκφραση

$$(z_1\frac{d}{dz_1})^0(z_2\frac{d}{dz_2})^1...(z_n\frac{d}{dz_n})^{n-1}D(z_1, ..., z_n)|_{z_1=...=z_n=1}. \tag{2}$$

Για να υπολογίσουμε την (2) θα χρησιμοποιήσουμε τον τύπο του Leibniz. Παρατηρούμε ότι εφαρμόζουμε $0+1+...+n-1 = \frac{n(n-1)}{2}$ παραγωγίσεις, δηλαδή όσο είναι και το πλήθος των γραμμικών παραγόντων $(z_j - z_{j'})$ του πολυωνύμου D. Τώρα, κάθε $z_j\frac{d}{dz_j}$ θα εξαλείφει κάποιον από τους γραμμικούς παράγοντες του z_j και θα τον αντικαθιστά με z_j ή θα παραγωγίζει το P. Τα $n-1$ αντίγραφα του $z_n\frac{d}{dz_n}$ μπορούν να εξαλείψουν $n-1$ γραμμικούς παράγοντες $(z_j - z_n)$ και σε κάθε έναν από αυτούς τους παράγοντες εφαρμόζουμε μονο μια φορά τον $z_n\frac{d}{dz_n}$. Συνολικά υπάρχουν $(n-1)!$ τρόποι που μπορεί αυτό να συμβει. Συνεχίζοντας την διαδικασία για τα $n-2$ αντίγραφα του $z_{n-1}\frac{d}{dz_{n-1}}$, θα έχουμε ότι εξαλείφουν $n-2$ γραμμικούς παράγοντες $z_j - z_{n-1}$ και υπάρχουν $(n-1)!$ τρόποι που μπορεί αυτό να συμβεί. Κάνοντας την ίδια διαδικασία για τα υπόλοιπα $z_k\frac{d}{dz_k}$ θα έχουμε ότι

$$(2) = (n-1)!(n-2)! \cdot ... \cdot 0! P(1, ..., 1)$$

Έχουμε ότι το $(n-1)!(n-2)!\cdot...\cdot 0!$ δεν είναι πολλαπλασιο του p και άρα αρκεί να δείξουμε ότι η (2) δεν είναι πολλαπλάσιο του p. Όμως εξ' ορισμού το D είναι η ορίζουσα ενός πίνακα που

έχει το στοιχείο $z_j^{\xi_k}$ στην θέση (j,k). Δηλαδή $D(z_1,...,z_n) = det\begin{bmatrix} z_1^{\xi_1} & .. & z_1^{\xi_n} \\ .. & .. & .. \\ z_n^{\xi_1} & .. & z_n^{\xi_n} \end{bmatrix}$. Οπότε για να υπολογίσουμε την (2) θα πολλαπλασιάσουμε την $l+1$ γραμμή της ορίζουσας με $(z_l\frac{d}{dz_j})^{l-1}$, για $1 \leq l \leq n$. Το αποτέλεσμα, θα είναι η ορίζουσα $det\begin{bmatrix} (z_1\frac{d}{dz_1})^0 z_1^{\xi_1} & .. & (z_1\frac{d}{dz_1})^0 z_1^{\xi_n} \\ .. & .. & .. \\ (z_n\frac{d}{dz_n})^{n-1} z_n^{\xi_1} & .. & (z_n\frac{d}{dz_n})^{n-1} z_n^{\xi_n} \end{bmatrix}$ όταν $z_1 = ... = z_n = 1$ που τελικα είναι ίση με $det\begin{bmatrix} 1 & .. & 1 \\ \xi_1 & .. & \xi_n \\ .. & .. & .. \\ \xi_1^{n-1} & .. & \xi_n^{n-1} \end{bmatrix}$. Αυτή η ορίζουσα είναι γνωστή ως η ορίζουσα Vandermonde και ισούται με

$$\pm \prod_{1 \leq k < k' \leq n} (\xi_k - \xi_{k'})$$

Όμως από την υπόθεση έχουμε ότι τα ξ_k είναι διαφορετικά $(mod p)$ μεταξύ τους, άρα η ορίζουσα δεν είναι μηδεν οπότε η (2) δεν είναι πολλαπλάσιο του p. Άρα και $P(1,...,1)$ δεν είναι πολλαπλλάσιο του p και οπότε από το προηγούμενο Λήμμα $P(\omega_1,...,\omega_n)$ δεν είναι μηδέν, δηλαδή

$$det(\omega_j^{\xi_k})_{1 \leq j,k \leq n}$$

είναι διάφορη του μηδέν. □

Ένα άμεσο πόρισμα είναι το εξής.

Το πόρισμα 2.4.

Πόρισμα 2.4. *Έστω p πρώτος και A, $\tilde{A}$ μη κενά υποσύνολα του Z_p με $|A| = |\tilde{A}|$. Ο γραμμικός μετασχηματισμός $T : l^2(A) \to l^2(\tilde{A})$ με $Tf = \hat{f}|_{\tilde{A}}$ είναι αντιστρέψιμος.*

Απόδειξη. Ο πίνακας T έχει την μορφή $(e^{2\pi i \chi_j \xi_k / p})_{1 \leq j,k \leq n}$ ως προς τη συνηθισμένη βάση και άρα από το προηγούμενο Λήμμα είναι αντιστρέψιμος. □

Τώρα είμαστε έτοιμοι να αποδείξοουμε το θεώρημα.

Απόδειξη. (του θεωρήματος 2.1) Έστω ότι υπάρχει μια μη μηδενική συνάρτηση f τέτοια ώστε $|supp(f)| + |supp(\hat{f})| \leq p$. Τότε αν θέσουμε $A = supp(f)$ μπορούμε να βρούμε ένα σύνολο $\tilde{A}$ υποσύνολο Z_p που να είναι ξένο ως προς τον φορέα της $\hat{f}$, $supp(\hat{f})$ και να έχει τάξη ίση με την τάξη της A, δηλαδή $|A| = |\tilde{A}|$. Αυτό γίνετε διότι $\hat{f} : Z_p \to C$ και $|\tilde{A}| + |supp(\hat{f})| \leq p$. Άρα, έχουμε ότι $Tf = \hat{f}|_{\tilde{A}} = 0$ και f όχι η μηδενική, οπότε καταλήξαμε σε αντίφαση του πορίσματος (2.4).
Για το αντίστροφο, πρώτα θα δείξουμε την περίπτωση όπου $|A| + |B| = p + 1$. Όπως πριν διαλέγουμε ένα υποσύνολο του Z_p, έστω $\tilde{A}$ (από την μεριά του φάσματος) με $|\tilde{A}| = |A|$ τέτοιο ώστε να τέμνει το B σε ένα μόνο σημείο, έστω ξ. Τότε από το πόρισμα, ο T είναι αντιστρέψιμος, και πιο συγκεκριμένα μπορούμε να βρούμε μια $f \in l^2(A)$ μη μηδενική ώστε ο μετασχηματισμος Fourier της, $\hat{f}$ να μηδενιζεται στο $\tilde{A} - \{\xi\}$ και είναι μη μηδενική στο ξ $(\tilde{A}, B \subseteq Z_p)$. Όμως από υπόθεση έχουμε ότι $|A| + |B| = p + 1$ και έχουμε $f \in l^2(A)$ άρα $|supp(f)| \leq |A|$. Επίσης έχουμε ότι $|supp(\hat{f})| \leq p - |A|$. Από το ευθύ του θεωρήματος έχουμε ότι $|supp(f)| + |supp(\hat{f})| \geq p+1$ άρα αναγκαστηκά $|supp(f)| = |A|$ και $|supp(\hat{f})| = |B|$.

Αν έχουμε ότι $|A|+|B| > p+1$, τότε, αν πάρουμε A', B' υποσύνολα των A και B αντίστοιχα, τέτοια ώστε $|A'|+|B'| = p+1$ θα υπάρχει f με $supp(f) = A$, $supp(\tilde{f}) = B$. Αν τώρα τον γραμμικό συνδιασμό των f_i (με κατάλληλες σταθερές) καθώς τα A' και B' ποικίλουν, τότε έπεται το αποτέλεσμα. Δηλαδή υπάρχει f με $|supp(f)| = |A|$ και $|supp(\hat{f})| = |B|$. □

Αξίζει να σημειώσουμε ότι εμείς στην συνέχεια θα χρειαστούμε το πόρισμα 2.4 και όχι το κυρίως θεώρημα. Το θεώρημα καθώς και η αποδειξή του περιλαμβάνονται εδώ για πληρότητα. Παρακάτω δίνονται μερικές εφαρμογές του θεωρήματος.

Εφαρμογές.

Εφαρμογή 2.5. *Μια άμεση συνέπεια του θεωρήματος είναι ότι αν έχω ένα πολυώνυμο $\sum_{j=0}^{k} c_j z^{n_j}$ με $k+1$ μη μηδενικούς συντελεστές και $0 \leq n_0 < ... < n_k < p$ τότε αν περιοριστούμε στις p-οστές ρίζες της μονάδας, έχει το πολύ k ρίζες. Πράγματι όταν περιοριστούμε στις p-οστές ρίζες της μονάδας, ένα τέτοιο πολυώνυμο είναι ο μετασχηματισμός Fourier στο $\mathbb{Z}_p$ κάποιας συνάρτησης, της οποίας οφορέας έχει ακριβώς $k+1$ στοιχεία. Οπότε σύμφωνα με το προηγούμενο θεώρημα, ο φορέας του πολυωνύμου θα έχει τουλάχιστον $p+1-(k+1) = p-k$ p-οστές ρίζες της μονάδας. Άρα το πολυώνυμο θα έχει το πολύ k ρίζες.*

Εφαρμογή 2.6. *Μια άλλη εφαρμογή είναι η ανισότητα Cauchy-Davenport.*
Για κάθε δύο πεπερασμένα μη κενά υποσύνολα του $\mathbb{Z}_p$ έχουμε ότι για το σύνολο $A+B = \{a+b : a \in A, b \in B\}$ ότι

$$|A+B| \geq min(|A|+|B|-1, p).$$

Απόδειξη. Έστω δύο μη κενά σύνολα A και B. Μπορούμε να βρούμε δύο υποσύνολα X και Y του $\mathbb{Z}_p$ τέτοια ώστε $|X| = p+1-|A|$, $|Y| = p+1-|B|$ και $|X \cap Y| = max(|X|+|Y|-p, 1)$. Απλά παίρνουμε X και Y τέτοια ώστε $|X|+|A| = p+1$ και $|Y|+|B| = p+1$ και επίσης να έχουν ή ακριβώς ένα κοινό στοιχείο ή ακριβώς $|X|+|Y|-p$, δηλαδή με $P+2-|A|-|B|$ (τα A, B είναι μη κενά). Ο λόγος που το θέλουμε αυτό είναι για να ικονοποιηθεί το συμπέρασμα της εφαρμογής.

Τώρα, αφού $|A|+|X| = p+1$ και $|B|+|Y| = p+1$, από το θεώρημα (2.1) υπάρχουν συναρτήσεις f και g με $supp(f) = A$, $supp(\hat{f}) = X$, $supp(g) = B$ και $supp(\hat{g}) = Y$. Τότε ο φορέας της $f*g$ περιέχεται στο $|A+B|$ και επειδή έχουμε ότι $\widehat{f*g} = \hat{f} \cdot \hat{g}$ ο φορεας της $\widehat{f*g}$ θα είναι ίσος με $X \cap Y$. Οπότε από το θεώρημα (2.1) έχουμε ότι $|A+B|+|X \cap Y| \geq p+1$ όπου αν $|X \cap Y| = 1$ τότε έχουμε ότι $|A+B| \geq p$. Από την άλλη αν $|X \cap Y| = |X|+|Y|-p$ τότε $|A+B| \geq p+1-|X|-|Y|+p = p+1-p-1+|A|-p-1+|B|+p = |A|+|B|-1$. Άρα τελικά, σε κάθε περίπτωση έχουμε ότι

$$|A+B| \geq min(|A|+|B|-1, p).$$

□

Με τις παραπάνω εφαρμογές ουσιαστικά ολοκληρώσαμε με τα εισαγωγικά αυτής εδώ της εργασίας και στην συνέχεια θα αναπτύξουμε τις μεθόδους ακριβούς ανάκτησης ενός σήματος όταν το μήκος του σήματος είναι πρώτος αριθμός.

Ακριβή ανάκτηση σήματος με μήκος πρώτο αριθμό.

Σε αυτό το σημείο θα δείξουμε ότι αν το μήκος του σηματος μας f είναι πρώτος αριθμός και ο φορέας T του αρκετά μικρός, τότε μπορούμε να έχουμε ακριβή ανάκτηση του σήματος.

Έστω $f \in C^N$ ένα σήμα με μήκος N και έστω ότι γνωρίζουμε τους συντελεστες Fourier της f πάνω σε ένα σύνολο $\Omega \subset Z_N$. Δηλαδή $\hat{f}|_\Omega$ είναι γνωστό. Έπίσης, έστω ότι T ο φορέας

της f είναι ένα μικρό αλλά εν γένει άγνωστο υποσύνολο του Z_N. Στην περίπτωση που το μήκος N είναι πρώτος μπορούμε να ανακτήσουμε την f αν το T είναι σχετικά μικρο. Όπως προείπαμε για να αποδείξουμε το βασικό μας θεώρημα στην περίπτωση που το μήκος του σηματός μας είναι πρώτος αριθμός θα χρειαστούμε από τα παραπάνω, το πόρισμα 2.4.

Θεώρημα 2.7. *Έστω f ένα σήμα μήκους N με N να είναι πρώτος αριθμός. Επίσης, έστω $\Omega \subset Z_N$ και ότι ο φορέας της f είναι το σύνολο T, τέτοιο ώστε*

$$|T| \leq \frac{1}{2}|\Omega|$$

Τότε μπορουμε να ανακτήσουμε πλήρως και με μοναδικό τρόπο την f από τα Ω και $\hat{f}|\Omega$.

Αντίστροφα, αν το Ω είναι γνήσιο υποσύνολο του Z_N, δηλαδή το Ω δεν περιέχει όλες τις N συχνότητες, τότε υπάρχουν διαφορετικές συναρτήσεις f,g τέτοια ώστε να ισχύει ότι

$$|supp(f)|, |supp(g)| \leq \frac{1}{2}|\Omega| + 1$$

και $\hat{f}|_\Omega = \hat{g}|_\Omega$.

Απόδειξη. Έστω ότι $|T| \leq \frac{1}{2}|\Omega|$ και ότι υπάρχουν f, g τέτοιες ώστε $\hat{f}|_\Omega = \hat{g}|_\Omega$ με

$$|supp(f)|, |supp(g)| \leq \frac{1}{2}|\Omega|$$

. Τότε ο μετασχηματισμός Fourier της $f - g$ θα είναι μηδέν στο σύνολο Ω. Επίσης, θα έχουμε ότι $|supp(f-g)| \leq |\Omega|$. Άρα από το πόρισμα (2.4) θα έχουμε ότι $T_{supp(f-g)\to\Omega}$ είναι $1-1$ με $\hat{f}|_\Omega = \hat{g}|_\Omega$. Όπότε τελικά θα έχουμε ότι $f - g = 0$, δηλαδή ότι $f = g$ που είναι άτοπο.
Αντίστροφα, αφού έχουμε ότι $|\Omega| < N$, μπορούμε να βρούμε δύο ξένα σύνολα, T, S, τέτοια ώστε να ισχύει ότι $|T|, |S| \leq \frac{1}{2}|\Omega|+1$ και $|T|+|S| = |\Omega|+1$. Έστω τώρα ω_0 μια συχνότητα που δεν ανήκει στο Ω. Πάλι, από το πόρισμα (2.4) θα έχουμε ότι ο $T_{T\cup S\to\Omega\cup\{\omega_0\}}$ είναι $1-1$ και επί. Αν πάρουμε τώρα ένα διάνυσμα h με φορέα στο σύνολο $T \cup S$ και με τον μετασχηματισμό Fourier του να είναι μηδέν στο Ω αλλά όχι στο ω_0, οπότε το h δεν είναι ταυτοτικά μηδέν, τότε, για $f = h|_T$ και $g = -h|s$ θα έχουμε ότι

$$|supp(f)|, |supp(g)| \leq \frac{1}{2}|\Omega| + 1$$

και $\hat{f}|_\Omega = \hat{g}|_\Omega$, που ήταν και το ζητούμενο. □

Με το παραπάνω θεώρημα είδαμε ποιες συνθήκες θα πρέπει να ικανοποιούνται ώστε να έχουμε μοναδική ανάκτηση ενός σήματος, όταν το μήκος του σήματος είναι πρώτος αριθμός. Δυστυχώς η συγκεκριμένη μέθοδος αποτυγχάνει στην περίπτωση που το μήκος του σήματος δεν είναι πρώτος αριθμός, καθώς παύει να ισχύει το πόρισμα 2.4 και άρα και το θεώρημα 2.7. Στην συνέχεια θα δούμε ένα αντιπαράδειγμα, όπου το T είναι αρκετά μικρό αλλά το μήκος του σήματος δεν είναι πρώτος και δεν μπορούμε να ανακτήσουμε το σήμα.

Αντιπαράδειγμα 2.8. *(o discrete Dirac comb.) Έστω ότι το N είναι τέλειο τετράγωνο και έστω ένα σήμα που στα πολλαπλάσια του $\sqrt{N}$ παίρνει την τιμή ένα ενώ παντού αλλού είναι μηδέν. Το συγκεκριμένο σήμα ονομάζεται discrete Dirac comb και έχει την ιδιότητα να παραμένει αναλλοίωτο από τον μετασχηματισμό Fourier. Έτσι, αν πάρουμε για Ω το σύνολο που περιέχει όλες τις συχνότητες εκτός τα πολλαπλάσια του $\sqrt{N}$ θα έχουμε ότι $\hat{f}|_\Omega \equiv 0$ και άρα δεν μπορούμε να ανακτήσουμε το σήμα.*

Στο επόμενο κεφάλαιο θα αναπτύξουμε τις μεθόδους ακριβούς ανάκτησης ενός σήματος γνωρίζοντας μόνο ένα μέρος των συχνοτήτων. Όπως προαναφέραμε η προσέγγιση του προβλήματος είναι πιθανοθεωρητική.

ΚΕΦΑΛΑΙΟ 3

Ακριβής ανάκτηση σήματος με μεγάλη πιθανότητα.

Εισαγωγή.

Παραπάνω είδαμε τι γίνεται όταν το μήκος του σηματός μας είναι πρώτος αριθμός, αλλά και γιατί αποτυγχάνει αυτή η προσέγγιση, με ένα παράδειγμα, όταν το μήκος δεν είναι πρώτος αριθμός. Είναι εύλογο να εξετάσουμε αν το πόρισμα 2.4 εξακολουθεί να ισχύει όταν το N δεν είναι πρώτος αριθμός και εάν τα T και Ω δεν είναι υποομάδες του Z_N αλλά ισχύουν κάποιες άλλες προυποθέσεις. Όπως θα δούμε, αν επιλέξουμε τα T και Ω τυχαία και ομοιόμορφα, τότε μπορούμε να ανακτήσουμε το σήμα μας με μεγάλη πιθανότητα.

Γενικά, ο πιο απλός τρόπος για να έχουμε ακριβή ανάκτηση της f είναι λύνοντας το παρακάτω πρόβλημα συνδυαστικής βελτιστοποίησης

$$(P_0) min_{g\in C^N} ||g||_{l_0}, \hat{g}|_\Omega = \hat{f}|_\Omega$$

όπου $||g||_{l_o}$ είναι ο αριθμός των μη μηδενικών όρων, δηλαδή το πλήθος όλων των στοιχείων t με $g(t) \neq 0$. Όπως είπαμε αυτό είναι ένα πρόβλημα συνδυαστικής βελτιστοποίησης και το να προσπαθήσουμε απευθείας να λύσουμε το (P_0) είναι υπολογιστικά ανέφικτο ακόμα και για μέτριου μεγέθους σήματα. Ουσιαστικά αυτό που θα πρέπει να κάνουμε για να λύσουμε το (P_0) είναι να αφήσουμε το T να ποικίλλει πάνω από όλα τα υποσύνολα του $\{0, ..., N-1\}$ και το πλήθος των στοιχείων του T να είναι το πολύ το μισό του Ω, δηλαδή $|T| \leq \frac{1}{2}|\Omega|$. Στην συνέχεια για κάθε ένα τέτοιο T θα πρέπει να τσεκάρουμε αν η $\hat{f}|_\omega$ αντιστρέφεται ή όχι και να πάρουμε τον αντίστροφο του αντιστοιχου Fourier minor του πίνακα Fourier για να ανακτήσουμε την f. Όπως είπαμε, αυτή η προσέγγιση είναι πρακτικά ανέφικτη μιας και έχει τεράστιο "υπολογιστικό κόστος" λόγω του μεγάλου πλήθους των δυνατών συνόλων T.

Μια πιο αποδοτική μέθοδος για να ανακτήσουμε την f από τα Ω και $\hat{f}|_\Omega$ είναι να λύσουμε το παρακάτω πρόβλημα βελτιστοποίησης:

(P_1) $min_{g\in C^N} ||g||_{l_1} := \sum_{t\in Z_N} |g(t)|$, $\hat{g}|_\Omega = \hat{f}|_\Omega$

Το κρίσιμης σημασίας αποτέλεσμα είναι ότι οι λύσεις (P_0) και (P_1) είναι ισοδύναμες για ένα μεγάλο ποσοστό επιλογών για τα T και Ω. Ειδικότερα θα δούμε ότι για $|T| \leq \alpha|\Omega|/\log N$, όπου α είναι μια σταθερά, λύνοντας το (P_1) μπορούμε να έχουμε ακριβή ανάκτηση του σήματός μας.

Τώρα θα παρουσιάσουμε το βασικό θεώρημα αυτής της εργασίας. Κατ' αρχήν θα θεωρήσουμε ότι οι συντεταγμένες Fourier που γνωρίζουμε είναι τυχαία κατανεμημένες και δεδομένου του αριθμού N_ω των συχνοτήτων που γνωρίζουμε παίρνουμε το Ω διαλέγοντας τυχαία N_ω συχνότητες. Δηλαδή συνολικά έχουμε $\binom{N}{N_\omega}$ πιθανά υποσύνολα όπου κάθε ένα από αυτά μπορεί να επιλεγεί με την ίδια πιθανότητα. Τώρα είμαστε έτοιμοι να παρουσιάσουμε το βασικό μας θεώρημα.

Το βασικό θεώρημα.

Θεώρημα 3.1. *Έστω $f \in C$ ένα διακριτό σήμα με φορέα πάνω σε ένα άγνωστο σύνολο T και έστω το σύνολο Ω με $|\Omega| = N_\omega$ που το επιλέγουμε με τυχαία ακολουθώντας την*

ομοιόμορφη κατανομή. Για δεδομένη παράμετρο ακρίβειας M αν

$$|T| \leq C_M \left(\log N\right)^{-1} |\Omega| \tag{3}$$

τότε η λύση του $(P1)$ είναι μοναδική και ίση με την f με πιθανότητα τουλάχιστον $1 - O\left(N^{-M}\right)$.

Παρατηρήστε ότι η (3) ουσιαστικά μας λέει ότι όταν ο φορεας T της f είναι της τάξης του Ω εκτός από μια σταθερά και ένα λογαριθμικό παράγοντα τότε ουσιαστικά δεν χάνουμε πληροφορίες, δηλαδή μπορούμε να έχουμε ακριβή ανάκτηση της f. Επίσης, από την άλλη το θεώρημα επιτρέπει να υπάρχουν f τέτοιες ώστε ακόμα και αν ο φορέας $|supp(f)|$ είναι πολύ μικρός συγκριτικά με το $|\Omega|$ να μην μπορούμε να τις ανακτήσουμε. Ένα τέτοιο παράδειγμα είναι το αντιπαράδειγμα 2.8 που είδαμε στο προηγούμενο κεφάλαιο.

Οπότε, τελικά, το θεώρημα 3.1 μας λέει ότι για τα περισσότερα σύνολα T που έχουν μέγεθος σχεδόν σαν το μέγεθος του Ω, δεν χάνουμε πληροφορίες στην ανάκτηση της f. Τώρα, για να αποδείξουμε το παραπάνω θεώρημα θα χρειαστει να αποδείξουμε μια σειρά απο λήμματα και πορίσματα καθώς και να χρησιμοποιήσουμε διάφορα εργαλεία που θα αναπτύξουμε στην συνέχεια.

Το τριγωνομετρικό πολυώνυμο P.

Σε αυτήν την παράγραφο θα δείξουμε ότι η f είναι η μοναδική μας λύση αν και μόνο αν υπάρχει ένα τριγωνομετρικό πολυώνυμο με δεδομένες ιδιότητες, τις οποίες θα αναπτύξουμε πλήρως.

Έστω T ο φορέας της f και έστω ότι γνωρίζουμε την $\hat{f}$ σε ένα σύνολο Ω. Το παρακάτω λήμμα ουσιαστικά μας λέει ότι μια ικανή και αναγκαία συνθήκη για την f ώστε να είναι η λύση του $(P1)$ είναι η ύπαρξη ενός τριγωνομετρικού πολυωνύμου P του οποίου ο φορέας του μετασχηματισμού Fourier περιέχεται στο Ω, $P(t) = sgn(f)$ στο T και στο συμπλήρωμα του T είναι μικρότερο από την μονάδα.

Λήμμα 3.2. *Έστω $\Omega \in Z_N$, $f \in C^N$ και T ο φορέας του f. Ορίζουμε $sgn(f(t)) = f(t)/|f(t)|$ όταν $t \in T$ και $sgn(f) = 0$ διαφορετικά. Αν υποθέσουμε επίσης ότι υπάρχει ένα διάνυσμα P τέτοιο ώστε ο φορέας του μετασχιματισμού Fourier $\hat{P}$ να είναι στο Ω και*

$$P(t) = sgn(f)(t) \tag{4}$$

για κάθε t στο T και

$$|P(t)| < 1 \tag{5}$$

για κάθε t στο συμπλήρωμα του T
τότε
αν ο $F_{T\to\Omega}$ είναι $1-1$, τότε η λύση του (P_1) είναι μοναδική και ίση με f.
Αντίστροφα, αν f είναι η μοναδική λύση του (P_1), τότε υπάρχει ένα διάνυσμα P με τις παραπάνω ιδιότητες. (Ο $F_{T\to\Omega}$ είναι ένας τελεστής από το $l_2(T)$ στο $l_2(\Omega)$ με $F_{T\to\Omega}(f) = \hat{f}|_\Omega$)

Απόδειξη. Αρχικά θα υποθέσουμε ότι το Ω είναι μη κενό και ότι η f όχι παντού μηδεν. Διαφορετικά η απόδειξη είναι προφανής.
Έστω τώρα ότι υπάρχει ένα τέτοιο πολυώνυμο P. Αν g είναι ένα διάνυσμα με $g \neq f$ και $\hat{g}|_\Omega = \hat{f}|_\Omega$ και θέσουμε $h = g - f$, τότε θα έχουμε ότι $\hat{h} \equiv 0$ στο Ω. Τότε για κάθε $t \in T$ θα έχουμε ότι

$$\begin{aligned} |g(t)| &= |f(t) + h(t)| \\ &= ||f(t)| + h(t)\overline{sgn(f(t))}| \end{aligned}$$

$$\geq |f(t)| + Re(h(t)\overline{sgn(f(t))})$$
$$= |f(t)| + Re(h(t)\overline{P(t)}).$$

Η δεύτερη ισότητα βγαίνει απλά τετραγωνίζοντας, ενω στη συνέχεια χρησιμοποιούμε στοιχειώδεις ιδιότητες μιγαδικών και ότι για $t \in T$ έχουμε ότι $P(t) = sgn(f(t))$.
Τώρα για $t \notin T$ έχουμε ότι $f \equiv 0$ και $P(t) < 1$. Άρα

$$|g(t)| = |h(t)| \geq Re(h(t)\overline{P(t)})$$

Οπότε τελικά θα έχουμε ότι

$$||g||_{l_1} \geq ||f||_{l_1} + \sum_{t=0}^{N-1} Re(h(t)\overline{P(t)}).$$

Όμως από τον τύπο του Parseval θα πάρουμε ότι

$$\sum_{t=0}^{N-1} Re(h(t)\overline{P(t)}) = \frac{1}{N}\sum_{k=0}^{N-1} Re(\hat{h}(k)\overline{\hat{P}(k)}) = 0$$

διότι ο φορέας του $\hat{P}$ είναι στο Ω ενώ όπως είπαμε παραπάνω $\hat{h}|_\Omega = 0$. Άρα έχουμε ότι $||g||_{l_1} \geq ||f||_{l_1}$ και θα εξετάσουμε πότε ισχύει η ισότητα, δηλαδή πότε έχουμε ότι $||g||_{l_1} = ||f||_{l_1}$. Γυρνώντας πίσω βλέπουμε ότι για να ισχύει η ισότητα θα πρέπει όταν $t \notin T$ να έχουμε ότι $|h(t)| = Re(h(t)\overline{P(t)})$. Επειδή όμως για $t \notin T$ έχουμε ότι $|P(t)| < 1$, θα έχουμε αναγκαστικά ότι $h \equiv 0$ στο συμπλήρωμα του T. Επίσης επειδή η $\hat{h}$ είναι μηδέν στο Ω και επειδή ο $F_{T\to\Omega}$ είναι 1-1 από την υπόθεση μας, αναγκαστικά η h θα είναι μηδέν παντού και οπότε θα έχουμε ότι $g = f$ και άρα η f είναι η μοναδική μας λύση στο $(P1)$.

Αντίστροφα, έστω ότι η f είναι η μοναδική λύση του $(P1)$. Χωρίς βλάβη της γενικότητας και για απλότητα ας υποθέσουμε ότι $||f||_{l_1} = 1$. Τότε η κλειστή μοναδιαία μπάλα $B = \{g : ||g||_{l_1} \leq 1\}$ και ο αφινικός χώρος $V = \left\{g : \hat{g}|_\Omega = \hat{f}|_\Omega\right\}$ τέμνονται σε ένα ακριβώς σημείο, την f. Από το θεώρημα Hahn-Banach υπάρχει μια συνάρτηση P τέτοια ώστε το υπερεπίπεδο $\Gamma_1 = \left\{g : \sum Re(g(t)\overline{P(t)}) = 1\right\}$ να περιέχει τον V και ο ημίχωρος $\Gamma_{\leq 1} = \left\{g : \sum Re(g(t)\overline{P(t)}) \leq 1\right\}$ να περιέχει την μπάλα B. Επειδή τα B και V έχουν μόνο ένα κοινό σημείο μπορούμε να υποθέσουμε ότι η τομή $\Gamma_1 \cap B$ περιέχει μια ακμή του πολυτόπου B που περιέχεται την f το οποίο είναι $\{g \in B : supp(g) \subseteq T\}$.
Τώρα, αφού το $\Gamma_{\leq 1}$ περιέχει το B θα έχουμε ότι $sup_t|P(t)| \leq 1$. Επίσης επειδή $f \in \Gamma_1 \cap B$ έχουμε ότι $P(t) = sgn(f(t))$ για $t \in supp(f)$. Επειδή το $\Gamma_1 \cap B$ περιέχεται στην παραπάνω ακμή, θα έχουμε ότι $|P(t)| < 1$ για $t \notin T$. Τέλος επειδή το V περιέχεται στο Γ_1, από Parseval θα έχουμε ότι $\hat{P}$ έχει φορέα στο Ω. □

Παρακάτω θα δείξουμε ότι μπορούμε να ανακτήσουμε την f κατασκευάζοντας ένα συγκεκριμμένο πολυώνυμο P (που θα εξαρτάται από τα T και Ω) το οποίο θα ικανοποιεί την ισότητα (4) στο T από το παραπάνω λήμμα, ενώ με μεγάλη πιθανότητα θα ικανοποιεί και την ανισότητα (5) στο συμπλήρωμα του T.
Επιλέγουμε λοιπόν το πολυώνυμο P να είναι το εξής:

$$P = F_\Omega^* F_{T\to\Omega} \left(F_{T\to\Omega}^* F_{T\to\Omega}\right)^{-1} i^* sgn(f) \tag{6}$$

όπου $F_\Omega = F_{Z_N\to\Omega}$ είναι ο τελεστής $F : l^2(Z_N) \to l^2(\Omega)$ που στέλνει μια συνάρτηση στον μετασχηματισμό Fourier της, περιορισμένη στο Ω. (Με την έκφραση $l^2(A)$ εννοούμε όλες τις συναρτήσεις f που είναι μηδέν έξω από το A.)

Ο τελεστής $\iota : l^2(T) \to l^2(Z_N)$ επεκτείνει ένα διάνυσμα από το T στο Z_N βάζοντας μηδενικά έξω από το T ενώ ι^* είναι η δυική απεικόνιση του ι που περιορίζει την εικόνα του f στο T. Δηλαδή $\iota^* f = f|_T$.
Με βάση τα παραπάνω και αν υποθέσουμε ότι ο τελεστής $F_{T\to\Omega}$ είναι 1-1 (θα το αποδείξουμε παρακάτω) τότε το $F^*_{T\to\Omega}F_{T\to\Omega}$ αντιστρέφεται, οπότε είναι εύκολο να δούμε ότι το πολυώνυμο P είναι καλά ορισμένο με $P : l^2(\Omega) \to l^2(T)$ και οπότε ο φορέας του $\hat{P}$ είναι στο Ω, οπότε το P ικανοποιεί την προυπόθεση του παραπάνω λήμματος. Επίσης από την (6) έχουμε ότι όταν περιοριστούμε στο T έχουμε ότι $P(t) = sgn(f)(t)$ δηλαδή ικανοποιείται η (4). Για να το δούμε αυτό αρκεί να παρατηρήσουμε ότι $\iota^* F^*_\Omega = F^*_{T\to\Omega}$ οπότε θα έχουμε

$$i^*P(t) = F^*_{T\to\Omega}F_{T\to\Omega}\left(F^*_{T\to\Omega}F_{T\to\Omega}\right)^{-1}\iota^* sgn(f)(t) = \iota^* sgn(f)(t)$$

Για να ικανοποιηθούν οι προυποθέσεις του παραπάνω λήμματος μένει να δείξουμε την αντιστρεψιμότητα του $F^*_{T\to\Omega}F_{T\to\Omega}$ καθώς επίσης και την συνθήκη (5). Τα παραπάνω, καθώς και το βασικό μας θεώρημα θα τα αποδείξουμε πιθανοθεωρητικά ως εξής: Θα διαλέξουμε το Ω με ομοιόμορφη τυχαιότητα πάνω από όλα τα σύνολα μεγέθους N_ω τέτοιο ώστε $N_\omega \geq C_M^{-1}\cdot|T|\cdot\log N$ (όπως στο βασικό θεώρημα, το (3.1)), οπότε θα δείξουμε ότι ο $F^*_{T\to\Omega}F_{T\to\Omega}$ είναι αντιστρέψιμος με πιθανότητα $1 - O(N^{-M})$ και η συνθήκη (5), δηλαδή $P(t) < 1$ στο συμπλήρωμα του T, ισχύει, πάλι με πιθανότητα $1 - O(N^{-M})$.

Το μοντέλο Bernoulli.

Μέχρι τώρα έχουμε μιλήσει για το μοντέλο ομοιόμορφης τυχαιότητας όπου το σύνολο Ω ακολουθεί την ομοιόμορφη κατανομή. Ωστοσο στην συνέχεια, για απλότητα, θα ακολουθήσουμε το μοντέλο Bernoulli το οποίο θα παρουσιάσουμε παρακάτω, καθώς θα μας βοηθήσει να ξεπεράσουμε καποια προβλήματα που εμφανίζονται στο μοντέλο της ομοιόμορφης τυχαιότητας όπως για παράδειγμα ο υπολογισμός της πιθανότητα μιας συχνότητας να είναι στο Ω, καθώς εξαρτάται από το εάν κάθε άλλη συχνότητα ανήκει στο Ω η όχι.

Για να πάρουμε το Ω', το σύνολο των συντελεστών Fourier με το μοντέλο Bernoulli με παράμετρο $0 < \tau < 1$, θα πρέπει πρώτα να πάρουμε την παρακάτω γνωστή ακολουθία: $I_\omega = 0$ με πιθανότητα $1-\tau$ και $I_\omega = 1$ με πιθανότητα 1 και στην συνέχεια να θέσουμε $\Omega' = \{\omega : I_\omega = 1\}$. Το μέγεθος του Ω' είναι τυχαίο καθώς ακολουθεί την διωνυμική κατανομή και επομένως η αναμενόμενη τιμή του Ω' θα είναι $E(|\Omega'|) = \tau N$.

Τέλος, αποδεικνύεται[4] ότι αν ισχύουν αυτά που θα κάνουμε παρακάτω με το μοντέλο Bernoulli, τότε ισχύουν και με το μοντέλο ομοιόμορφης τυχαιότητας, οπότε από εδώ και πέρα θα δουλέψουμε με αυτό το μοντέλο.

Οι βοηθητικοί πίνακες H και H_0.

Σε αυτό το σημείο θα παρουσιάσουμε δύο πίνακες που θα μας βοηθήσουν να γράψουμε το πολυώνυμο P σε μια διαφορετική, πιο απλή μορφή. Έστω

$$Hf(t) = -\sum_{\omega\in\Omega}\sum_{t'\in T:t'\neq t} e^{2\pi i\frac{\omega(t-t')}{N}} f(t')$$

και ορίζουμε $H_0 = \iota^* H$. Έχουμε ότι

$$\iota - \frac{1}{|\Omega|}H = \frac{1}{|\Omega|}F^*_\Omega F_{T\to\Omega}$$

και πολλαπλασιάζοντας με ι^*

$$I_T - \frac{1}{|\Omega|}H_0 = \frac{1}{|\Omega|}F^*_{T\to\Omega}F_{T\to\Omega}$$

όπου $I_T = \iota^*\iota$ η ταυτότητα στο $l^2(T)$. Άρα το P γράφεται:

$$P = \left(\iota - \frac{1}{|\Omega|}H\right)\left(I_T - \frac{1}{|\Omega|}H_0\right)^{-1}\iota^* sgnf. \tag{7}$$

Οπότε για την αντιστρεψιμότητα του $F^*_{T\to\Omega}F_{T\to\Omega}$ αρκεί να δείξουμε ότι ο πίνακας $I_T - \frac{1}{|\Omega|}H_0$ είναι αντιστρέψιμος με μεγάλη πιθανότητα. Αυτό θα το κάνουμε δείχνοντας ότι κάποια νόρμα του τελεστή H_0 (για παράδειγμα η μεγαλύτερη ιδιοτιμή) είναι μικρότερη από $|\Omega|$.

Αντιστρεψιμότητα.

Ένας άμεσος τρόπος να το αποδείξουμε είναι φράζοντας την νόρμα του H_0 από την νόρμα του Frobenius $||H_0||_F$ (Η Frobenius νόρμα ορίζεται ως εξής: $||H_0||_F = Tr(H_0H_0^*) = \sum_{t_1,t2}|(H_0)_{t_1,t2}|^2$, δηλαδή είναι το άθροισμα των τετραγώνων όλων των στοιχείων του πίνακα.) Όπως είπαμε παραπάνω ο H_0 είναι αυτοσυζυγής (και άρα διαγωνιοποιήσιμος) όποτε θα έχουμε $||H_0||^{2n} = ||H_0^n||^2 \le ||H_0^n||_F^2 = Tr(H_0^n(H_0^*)^n) = Tr(H_0^{2n})$. Έστω τώρα $0 < \alpha < 1$. Από την ανισότητα του Markov έχουμε ότι:

$$P\left(||H_0^n||_F \ge \alpha^n|\tau N|^n\right) \le \frac{E||H_0^n||_F^2}{\alpha^{2n}|\tau N|^{2n}} \tag{8}$$

Στην συνέχεια θα παρουσιάσουμε ένα θεώρημα το οποίο θα μας φανεί πολύ χρήσιμο αλλά επειδή η απόδειξη του είναι πολύ τεχνική θα την αφήσουμε για το τέλος της εργασίας και πιο συγκεκριμένα το τελευταίο κεφάλαιο αυτής της εργασίας έχει να κάνει με αυτήν την απόδειξη. Αφορά μία εκτίμηση η οποία θα παίξει σημαντικό ρόλο παρακάτω και γιάυτό το λόγο και θα την ονομάσουμε εκτίμηση κλειδί.

Θεώρημα 3.3. *Έστω ότι $\tau \le 1/(1+e)$, τότε με το μοντέλο Bernoulli έχουμε:*

- $$E[Tr(H_0^{2n})] \le 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}|\tau N|^n|T|^{n+1}$$
  όταν $n \le \frac{\tau N}{4(a-\tau)|T|}$
- $$E[Tr(H_0^{2n})] \le \frac{n}{1-\tau}(4n)^{2n-1}|\tau N||T|^{2n}$$
  διαφορετικά

Έστω τώρα ότι $\tau \le 1/(1+e)$ και $n \le \tau N/[4|T|(1-\tau)]$. Από το παραπάνω θεώρημα για την εκτίμηση κλειδί έχουμε για την $2n$ ροπή του H_0 ότι:

$$E(Tr(H_0^{2n})) \le 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}|\tau N|^n|T|^{n+1} \tag{9}$$

Δεδομένου ότι $||H_0^n||_F^2 = Tr(H_0^{2n})$ και χρησιμοποιώντας την (9), η (8) γίνεται:

$$P\left(||H_0^n||_F \ge \alpha^n|\tau N|^n\right) \le 2ne^{-n}\left(\frac{4n}{\alpha^2(1-\tau)}\right)^n\left(\frac{|T|}{|\tau N|}\right)^n|T| \tag{10}$$

Ο μόνος περιορισμός που έχουμε για το μέγεθος του T στην παραπάνω σχέση είναι από την (9). Στο παρακάτω θεώρημα θα αποδείξουμε ότι ο $I_T - \frac{1}{|\Omega|}H_0$ είναι αντιστρέψιμος με μεγάλη πιθανότητα περιορίζοντας κατάλληλα το μέγεθος του T.

Θεώρημα 3.4. *Έστω ότι $\tau \le (1+e)^{-1}$ και $|T| \le \frac{\alpha_M^2(1-\tau)}{4}\frac{|\tau N|}{n}$ με $\alpha_M \le \alpha \le 1$ τότε*

$$P\left(||H_0^n||_F \ge \alpha^n|\tau N|^n\right) \le \frac{1}{2}\alpha^2 e^{-n}|\tau N|$$

Οπότε βάζοντας για $n = (M+1)\log N$ το οποίο αντιστοιχεί στις υποθέσεις του βασικού μας θεωρήματος (θεώρημα 3.1) έχουμε ότι ο $I_T - \frac{1}{|\Omega|}H_0$ είναι αντιστρέψιμος με πιθανότητα τουλάχιστον $1 - 1.25N^{-M}$.

Απόδειξη. Άν βάλουμε το φράγμα που έχουμε για το T από την υπόθεση μας στην (10) παίρνουμε το ζητούμενο φράγμα για την νορμα Frobenius του H_0

$$P\left(||H_0^n||_F \geq \alpha^n |\tau N|^n\right) \leq \frac{1}{2}\alpha^2 e^{-n}|\tau N|$$

Τώρα, από το θεωρημα μεγάλης αποκλίσεως[5] έχουμε ότι $P(|\Omega| < E|\Omega| - t) \leq exp(-t^2/2E|\Omega|)$. Αν θέσουμε $\epsilon_M = \sqrt{\frac{2M\log N}{|\tau N|}}$ και $t = \epsilon_M|\tau N|$ από το παραπάνω θα έχουμε ότι

$$P(|\Omega| < E|\Omega| - \epsilon_M|\tau N|) \leq exp(-(\epsilon_M|\tau N|)^2/2E|\Omega|)$$

. Κάνοντας πράξεις και στα δύο μέλη έχουμε ότι

$$P(|\Omega| < |\tau N| - \epsilon_M|\tau N|) \leq exp(-\frac{2M\log N|\tau N|^2}{2|\tau N|^2})$$

οπότε τελικά θα έχουμε

$$P(|\Omega| < |\tau N| - \epsilon_M|\tau N|) \leq N^{-M}$$

Θέτουμε τώρα B_M να είναι το ενδεχόμενο $\{|\Omega| < (1-\epsilon_M)|\tau N|\}$ και για $n = (M+1)\log N$ και $\alpha = 1/\sqrt{2}$ θέτουμε $A_M = \left\{||H_0|| \geq |\tau N|\sqrt{2}\right\}$. Από το θεώρημα μεγάλης αποκλίσεως έχουμε ότι

$$P(A_M) \leq \frac{1}{2}\frac{1}{\sqrt{2}^2}e^{-(M+a)\log N}|\tau N| \leq \frac{1}{4}|\tau N|N^{-(M+1)} \leq \frac{1}{4}N^{-M}$$

και στο $A_M \cup B_M$ έχουμε ότι

$$||H_0|| < |\tau N|/\sqrt{2} \leq \frac{|\Omega|}{\sqrt{2}(1-\epsilon_M)}$$

και άρα $H_0 \leq |\Omega|$ με μεγάλη πιθανότητα οπότε ο $I_T - \frac{1}{|\Omega|}H_0$ είναι αντιστρέψιμος με μεγάλη πιθανότητα. □

Με την απόδειξη του παραπάνω θεωρήματος έχουμε δείξει ότι το P είναι καλά ορισμένο και μας μένει να δείξουμε ότι το P είναι μικρότερο της μονάδας στο συμπλήρωμα του T καθώς επίσης και να αποδείξουμε το θεώρημα 3.3 για την εκτίμηση κλειδί. Πριν όμως προχωρήσουμε θα δώσουμε μια καλύτερη εκτίμηση για την νόρμα του H_0.

Πόρισμα 3.5. *Έστω ότι $|T|\log|T| \leq \tau N/(4(1-\tau))$ και $\gamma = \sqrt{4/(1-\tau)}$. Γιακάθε $\epsilon > 0$ έχουμε ότι*

$$P(||H_0|| > (1+\epsilon)\gamma\sqrt{\log|T|}\sqrt{|T||\tau N|}) \to 0$$

καθώς $|T|$, $|\tau N| \to \infty$

Απόδειξη. Αν θέσουμε για $\lambda = \gamma\sqrt{\log|T|}\sqrt{|T||\tau N|}$ τότε από την ανισότητα Markov έχουμε ότι

$$P(||H_0|| \geq (1+\epsilon)\lambda) \leq \frac{E[Tr(H_0^{2n})]}{(1+\epsilon)^{2n}\lambda^{2n}} \tag{11}$$

και για $n = \log|T|$ έχουμε ότι $e^{-n}n^n|T| \leq (\log|T|^n)$ οπότε η (9) θα γίνει

$$E[Tr(H_0^{2n})] \leq 2\left(\frac{4}{1-\tau}\right)^n n|\tau N|^n|T|^n(\log T)^n$$

και άρα

$$E[Tr(H_0^{2n})] \leq 2n\lambda^{2n}$$

οπότε η (11) γίνεται:

$$P(||H_0|| \geq (1+\epsilon)\lambda) \leq \frac{2n\lambda^{2n}}{(1+\epsilon)^{2n}\lambda^{2n}} = \frac{2n}{(1+\epsilon)^{2n}} \to 0$$

καθώς $n = \log|T| \to \infty$. □

Μια εκτίμηση για τις σειρές Neumann.

Σε αυτό το σημείο θα δείξουμε ότι με μεάλη πιθανότητα $|P(t)| < 1$ στο συμπλήρωμα του T. Πρώτα θα εκφράσουμε το $P(t)$ με έναν διαφορετικό τρόπο, χρησιμοποιώντας κάποιες αλγεβρικές ταυτότητες. Ποιο συγκεκριμένα, για ένα πίνακα M από την:

$$(I - M^n) = (I - M)\left(I + M + ... + M^{n-1}\right)$$

προκύπτει ότι:

$$(I - M)^{-1} = (I - M^n)^{-1}\left(I + M + ... + M^{n-1}\right)$$

Επίσης, υποθέτοντας σύγκλιση σε κάποια νόρμα τελεστή έχουμε ότι:

$$(I - M^n)^{-1} = \sum_{k=0}^{\infty} M^{nk}$$

Από τις δύο παραπάνω σχέσεις έχουμε ότι

$$\left(I_T - \frac{1}{|\Omega|^n}H_0^n\right)^{-1} = I_T + R$$

Όπου

$$R = \sum_{k=1}^{\infty} \frac{1}{|\Omega|^{kn}} H_0^{kn}$$

και άρα

$$\left(I_T - \frac{1}{|\Omega|}H_0\right)^{-1} = (I_T + R)\sum_{k=0}^{n-1} \frac{1}{|\Omega|^k} H_0^k. \tag{12}$$

Στην συνέχεια θα δείξουμε για τον όρο R ότι η νόρμα Frobenius και η άπειρο νόρμα είναι σχετικά μικρές. Έστω ότι $||i^*H||_F \leq a|\Omega|$ και επειδή $H_0 = i^*H$ θα έχουμε ότι

$$||R||_F = \sum_{k=1}^{\infty} \left|\left|\frac{H_0^{kn}}{|\Omega|^{kn}}\right|\right| = \sum_{k=1}^{\infty} \left|\left|\frac{(\iota^*H)^{kn}}{|\Omega|^{kn}}\right|\right| \leq \sum_{k=1}^{\infty} a^n = \frac{a}{1-a}$$

Έπίσης, όπως γνωρίζουμε, η άπειρο νόρμα ενός πίνακα είναι $||M||_\infty = sup_{||x||\leq 1}||Mx||_\infty = sup_i \sum_j |M(i,j)|$ οπότε από την Cauchy-Schwarz και κάνοντας πράξεις, θα έχουμε ότι

$$||M||_\infty^2 \leq sup_i|col(M)| \sum_j |M(i,j)|^2 \leq |col(M)| \sum_{i,j} |M(i,j)|^2 = |col(M)| \cdot ||M||_F^2$$

όπου $|col(M)|$ είναι το πλήθος των στηλών του M. Όποτε αφού ο H_0 (και άρα και ο R) έχει T στήλες, χρησιμοποιώντας τις δύο παραπάνω σχέσεις, έχουμε ότι:

$$||R||_\infty \leq |T|^{1/2}\frac{a}{1-a} \tag{13}$$

Αυτό που μένει, είναι να βρούμε ένα καλό φράγμα για την κομμένη σειρά Neuman $\frac{1}{|\Omega|}H\sum_{k=0}^{n-1}\frac{1}{|\Omega|^k}H_0^k$. Για να δούμε τώρα τι γίνεται στο συμπλήρωμα του T, που αυτό μας ενδιαφέρει, θα πρέπει να γυρίσουμε στην (7), η οποία υπενθυμίζουμε ότι είναι η:

$$P=\left(\iota-\frac{1}{|\Omega|}H\right)\left(I_T-\frac{1}{|\Omega|}H_0\right)^{-1}\iota^* sgnf.$$

και να παρατηρήσουμε ότι η (7) στο συμπλήρωμα του T παίρνει την μορφή:

$$P=\frac{1}{|\Omega|}H\left(I_T-\frac{1}{|\Omega|}H_0\right)^{-1}\iota^* sgnf,$$

αφού το ι είναι μηδέν στο συμπλήρωμα του T (στην πραγματικότητα στην παραπάνω ισότητα λείπει το πρόσημο το οποίο το παραλείψαμε συνηδειτά για απλότητα, μιας που δεν παίζει κανένα ρόλο). Αν θέσουμε τώρα $P_0=S_n sgn(f)$ και

$$P_1=\frac{1}{|\Omega|}HR\iota^*(I+S_{n-1})sgn(f)$$

όπου

$$S_n=\sum_{k=1}^{n}|\Omega|^{-k}(H\iota^*)^m$$

τότε για κάθε t στο συμπλήρωμα του T (μετά από πράξεις) έχουμε ότι $P(t)=P_0(t)+P_1(t)$ και η ιδέα είναι να βρούμε ένα φράγμα για τον κάθε όρο ξεχωριστά.

Έστω α_0,$\alpha_1>0$ δυο αριθμοί τέτοιοι ώστε $\alpha_0+\alpha_1=1$. Τότε θα έχουμε ότι

$$P(sup_{t\in T^c}|P(t)|>1)\leq P(||P_0||_\infty>\alpha_0)+P(||P_1||_\infty>\alpha_1)$$

και άρα αρκεί να δείξουμε ότι το δεξιό μέλος με μεγάλη πιθανότητα γίνεται αρκετά μικρο. Αν θέσουμε τώρα $Q_0=S_{n-1}sgn(f)$ (παρατηρείστε ότι το Q_0 και το P_0 διαφέρουν κατά ένα όρο) θα έχουμε ότι $P_1=\frac{1}{|\Omega|}HR(\iota^*sgn(f)+\iota^*Q_0)$ και άρα

$$||P_1||_\infty\leq\frac{1}{|\Omega|}||HR||_\infty(1+||\iota^*Q_0||_\infty)$$

οπότε για να ελεγξουμε την άπειρο νόρμα του P_1 αρκεί να ελέγξουμε τα $||HR||_\infty$ και $||\iota^*Q_0||_\infty$. Αυτό το κάνουμε διότι $||\iota^*Q_0||_\infty\leq||Q_0||_\infty$ μιας και το ι^* περιορίζει το Q_0 στο T και το Q_0 με το P_0 διαφέρουν κατά ένα όρο, δηλαδή έχουν σχεδόν τις ίδιες νόρμες τελικά, οπότε αρκεί να ελεγξουμε τις άπειρο νόρμες του P_0 και του HR. Έστω $t\in T^c$ σταθεροποιημένο. Τώρα θα ξαναγράψουμε το $P_0(t)$ ως $P_0(t)=\sum_{k=1}^{n}|\Omega|^{-k}X_k(t)$ με $X_k=(H\iota^*)^k sgn(f)$ και η ιδέα είναι να χρησιμοποιήσουμε εκτιμήσεις για τις ροπές για να ελέγξουμε το μέγεθος κάθε ενός από τα $X_k(t)$

Λήμμα 3.6. [6] *Έστω $n=km$. Τότε θα έχουμε ότι*

$$E|X_m(t_0)|^{2k}\leq 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}|\tau N|^n|T|^n$$

Δηλαδή έχουμε την ίδια εκτίμηση όπως στο θεώρημα 3.3 αλλά με την μόνη διαφορά ότι τώρα έχουμε και τον παράγοντα $|T|^{-1}$.

Απόδειξη. Η απόδειξη είναι ίδια με την απόδειξη του θεωρήματος 3.3 και θα την παραλείψουμε. □

Λήμμα 3.7. *Έστω* $a_0 = 0.91$ *και έστω όπως στο θεώρημα 3.4 ότι*

$$|T| \leq \frac{\alpha_M^2(1-\tau)}{4}\frac{|\tau N|}{n}.$$

Επίσης έστω ότι B_M *το σύνολο όπου* $|\Omega| < (a-\epsilon_M)|\tau N|$ *με* $\epsilon_M = \sqrt{2M\log N/|\tau N|}$. *Για κάθε* $t \in Z_N$ *υπάρχει ένα σύνολο* A_t *τέτοιο ώστε* $P(A_t) > 1-\epsilon_n$, *με*

$$\epsilon_n = 2(1-\epsilon_M)^{-2n}n^2e(-n)a^{2n}(0.42)^{-2n}$$

και $|P_0(t)| < 0.91$, $|Q_0(t)| < 0.91$ *στο* $A_t \cap B_M^c$. *Επομένως θα έχουμε ότι:*

$$P(sup_t|P_0(t)| > a_0) \leq N^{-M} + N\epsilon_n$$

και

$$P(sup_t|Q_0(t)| > a_0) \leq N^{-M} + N\epsilon_n$$

Απόδειξη. Για απλότητα θα θεωρήσουμε ότι το n είναι της μορφής $n = 2^J - 1$. Για κάθε m και k τέτοια ώστε $km \geq n$ και από τις

$$|T| \leq \frac{\alpha_M^2(1-\tau)}{4}\frac{|\tau N|}{n}$$

(όπως στο θεώρημα 3.4) και

$$E|X_m(t_0)|^{2k} \leq 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1}|\tau N|^n|T|^n$$

έχουμε ότι

$$E|X_m(t)|^{2k} \leq 2ne^{-n}a^{2n}|\tau N|^{2n} \tag{14}$$

Έχουμε ότι $|\Omega| \approx |\tau N|$ και όπως παραπάνω B_M^c το σύνολο που ισχύει ότι $|\Omega| \geq (1-\epsilon_M)|\tau N|$. Σε αυτό το σύνολο, και επειδή $P_0(t) = \sum_{m=1}^n |\Omega|^{-m}X_m(t)$ και $|1-\epsilon_M|^{-m}|\tau N|^{-m} < 1$ θα έχουμε ότι

$$|P_0(t)| \leq \sum_{m=1}^n Y_m,$$

όπου

$$Y_m = \frac{1}{(1-\epsilon_M)^m|\tau N|^m}|X_m(t)|.$$

Αν σταθεροποιήσουμε τώρα κάποια β_j, $0 \leq j \leq J$ τέτοια ώστε $\sum_{j=0}^{J-1} 2^j\beta j \leq a_0$ θα έχουμε ότι

$$P(\sum_{m=1}^n Y_m > a_0) \leq \sum_{j=0}^{J-1}\sum_{m=2^j}^{2^{j+1}-1} P(Y_m > \beta_j) \leq \sum_{j=0}^{J-1}\sum_{m=2^j}^{2^{j+1}-1} \beta_j^{-2K_j}E|Y_m|^{2K_j}$$

(από Markov) όπου $K_j = 2^{J-j}$. Τώρα, για κάθε m με $2^j \leq m \leq 2^{j+1}$ για το K_jm έχουμε ότι $n \leq K_jm < 2n$ οπότε από την (14) θα έχουμε ότι

$$E|Y_m|^{2K_j} \leq (1-\epsilon_M)^{-2mK_j}|\tau N|^{-2mK_j}2ne^{-n}a^{2n}|\tau N|^{2n}$$

οπότε θα έχουμε ότι

$$E|Y_m|^{2K_j} \leq (1-\epsilon_M)^{-2n}|\tau N|^{-2n}2ne^{-n}a^{2n}|\tau N|^{2n}$$

και τελικά

$$E|Y_m|^{2K_j} \leq 2(1-\epsilon_M)^{-2n}ne^{-n}a^{2n}.$$

Αν τώρα θεωρήσουμε ότι όλα τα $\beta_j^{-K_j}$ να είναι σταθερές για κάθε j π.χ. $\beta_j^{-K_j} = \beta_0^{-n}$ τότε θα έχουμε ότι

$$P(\sum_{m=1}^{n} Y_m > a_0) \leq 2(1-\epsilon_M)^{-2n} n^2 e^{-n} a^{2n} \beta_0^{-2n}.$$

Οπότε θα έχουμε ότι $P(sup_t|P_0(t)| > a_0) \leq 2(1-\epsilon_M)^{-2n} n^2 e^{-n} a^{2n} \beta_0^{-2n}$, δηλαδή αποδείξαμε το ζητούμενο. Η απόδειξη για το Q_0 είναι η ίδια. (Όπως έχουμε παρατηρήση τα P_0 και Q_0 διαφέρουν κατά μια σταθερά.) □

Μένει να δείξουμε ότι η άπειρο νόρμα του P_1 είναι μικρή μεμεγάλη πιθανότητα.

Λήμμα 3.8. *Έστω $a_1 = 0.91$ και έστω ότι τα a, n υπακούουν στην σχέση*

$$|T|^{3/2} \frac{a^n}{1-a^n} \leq a_1/2$$

. Τότε, στο ενδεχόμενο $A \cap \{||\iota^* H||_F \leq a|\Omega|\}$, για κάποιο A τέτοιο ώστε $P(A) \geq 1 - O(N^{-M})$ έχουμε ότι

$$||P_1||_\infty \leq a_1.$$

Απόδειξη. Όπως είδαμε προηγουμένος, $||P_1||_\infty \leq \frac{1}{|\Omega|}||H||_\infty ||R||_\infty (1 + ||Q_0||_\infty)$. Επίσης από το παραπάνω λήμμα, (3.7) έχουμε ένα φράγμα για το Q_0. Έστω τώρα το ενδεχόμενο $\{||Q_0||_\infty \leq 1\}$. Σε αυτό το ενδεχόμενο έχουμε ότι $||P_1||_\infty \leq a_1$ εαν $\frac{1}{|\Omega|}||H||_\infty ||R||_\infty \leq a_1/2$. Οπότε αρκεί να δείξουμε ότι $\frac{1}{|\Omega|}||H||_\infty ||R||_\infty \leq a_1/2$. Για τον πίνακα H έχουμε ότι έχει $|T|$ στήλες και κάθε στοιχείο του πίνακα είναι φραγμένο από το $|\Omega|$ άρα $||H||_\infty \leq |\Omega||T|$. Οπότε από την (13) που υπενθυμίζουμε ότι είναι η $||R||_\infty \leq |T|^{1/2} \frac{a^n}{1-a^n}$ έχουμε ότι

$$||H||_\infty ||R||_\infty \leq |T|^{3/2} \frac{a^n}{1-a^n}$$

με πιθανότητα τουλάχιστον $1 - O(N^{-M})$. Οπότε αρκεί να διαλέξουμε κατάλληλα τα a και n ώστε

$$|T|^{3/2} \frac{a^n}{1-a^n} \leq a_1/2$$

και επομένως για αυτά τα a και n θα έχουμε το ζητούμενο, δηλαδή ότι $||P_1||_\infty \leq a_1$. □

Με την απόδειξη αυτού του λήμματος ολοκληρώσαμε την απόδειξη του θεωρήματος 3.1 και κατ' επέκταση του βασικού θεωρήματος αυτής της εργασίας. Το μόνο που μένει για να είναι πλήρης είναι να παρουσιάσουμε και την απόδειξη του θεωρήματος 3.3 που την είχαμε αφήσει για το τέλος αυτής της εργασίας. Στο επόμενο κεφάλαιο παρουσιάζουμε βήμα βήμα αυτήν την δύσκολη και πολύ τεχνική απόδειξη.

ΚΕΦΑΛΑΙΟ 4

Η απόδειξη του θεωρήματος 3.3.

Εισαγωγή.

Σε αυτό το κεφάλαιο θα παρουσιάσουμε την απόδειξη του θεωρήματος 3.3. Όπως προαναφέραμε η απόδειξη αυτού του θεωρήματος είναι δύσκολη και τεχνική. Γιαυτό θα είναι προτιμότερο να σκιαγραφήσουμε την στρατηγική μας πριν προχωρήσουμε στη απόδειξη. Στην αρχή θα ξεκινήσουμε δίνοντας ένας πρώτο τύπο για την ποσότητα $E(Tr(H_0^{2n}))$. Αυτό θα μας επιτρέψει να φτιάξουμε έναν δεύτερο πιο χρήσιμο τύπο για την $E(Tr(H_0^{2n}))$. Στην συνέχεια θα αποδείξουμε το θεώρημα εκτιμόντας και φράζοντας κάποιες ποσότητες που θα εμφανιστούν καθώς εφαρμόζουμε τον δεύτερο τύπο στην απόδειξή μας.

Ο πρώτος τύπος για την αναμενόμενη τιμή του $Tr(H_0^{2n})$.

Όπως γνωρίζουμε ο πίνακας $H_0 = \iota^* H$ είναι διάστασης $|T| \times |T|$ με κάθε στοιχείο του πίνακα να παίρνει τιμές

$$H_0(t, t') = \mu(t - t')$$

όπου

$$\mu(t - t') = \sum_{\omega \in \Omega} e^{\frac{2\pi i}{N}\omega(t-t')}$$

όταν $t \neq t'$ και είναι μηδέν διαφορετικά. Οπότε χρησιμοποιώντας ότι $t_{2n+1} = t_1$, ένα στοιχείο της διαγωνίου του πίνακα H_0^{2n} θα είναι της μορφής

$$H_0^{2n}(t_1, t_1) = \sum_{t_2,\ldots,t_{2n}: t_j \neq t_{j+1}} \mu(t_1 - t_2)...\mu(t_{2n} - t_1)$$

Οπότε για την εκτίμηση του $E[Tr(H_0^{2n})]$ θα έχουμε ότι

$$E(Tr(H_0^{2n})) = \sum_{t_1,t_2,\ldots,t_{2n}: t_j \neq t_{j+1}} E\left[\sum_{\omega_1,\ldots,\omega_{2n} \in \Omega} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n} \omega_j (t_j - t_{j+1})}\right].$$

Χρησιμοποιώντας την γραμμικότητα της εκτίμησης και από το μοντέλο Bernoulli ότι $\Omega' = \{\omega : I_{\omega=1}\}$ θα έχουμε

$$E(Tr(H_0^{2n})) = \sum_{t_1,t_2,\ldots,t_{2n}: t_j \neq t_{j+1}} \sum_{0 \leq \omega_1,\ldots,\omega_{2n} \leq N-1} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n} \omega_j (t_j - t_{j+1})} E\left[\prod_{j=1}^{2n} I_{\{\omega_j \in \Omega\}}\right]. \quad (15)$$

Ο σκοπός μας είναι να χρησιμοποιήσουμε την ανεξαρτησία των $I_{\omega_j \in \Omega}$ για να απλοποιήσουμε την παραπάνω σχέση. Το πρόβλημα όμως εγκειται στο ότι κάποια από τα ω_j ίσως είναι τα ίδια, με αποτέλεσμα να χάνεται η ανεξαρτησία. Για να ξεπεράσουμε αυτήν τη δυσκολία θα πρέπει να εισάγουμε έναν καινούργιο συμβολισμό.

Έστω $Z_N = \{0, 1, ..., N-1\}$ το σύνολο όλων των συχνοτήτων και $A = \{1, 2, ..., 2n\}$. Για κάθε $\omega = (\omega_1, ..., \omega_{2n})$ ορίζουμε μια σχέση ισοδυναμίας $\sim_\omega$ στο A ως εξής. Θα λέμε ότι δύο δείκτες j και j' είναι ισοδύναμοι $j \sim \omega j'$ στο A αν και μόνο αν $\omega_j = \omega_{j'}$ και εστω τώρα $P(A)$ να είναι το σύνολο όλων των κλάσεων ισοδυναμίας στο A. Παρατηρήστε ότι

με αυτήν την σχέση ισοδυναμίας έχουμε μερική διάταξη, δηλαδή, $\sim_1 \leq \sim_2$ αν η $\sim_1$ είναι πιο χονδροειδής από την $\sim_2$ που σημαίνει ότι αν $a \sim_2 b$ τότε $a \sim_1 b$, για κάθε $a, b \in A$. Οπότε η πιο χονδροειδής σχέση ισοδυναμίας είναι αυτή όπου όλα τα στοιχεία του A είναι ισοδύναμα μεταξύ τουε ενώ η πιο λεπτή είναι αυτή όπου κάθε στοιχείο του A αποτελεί και μια κλάση ισοδυναμίας. Σε αυτήν την περίπτωση είναι προφανές ότι θα έχουμε ακριβώς $|A|$ κλάσεις ισοδυναμιας.

Τώρα, για κάθε σχέση ισοδυναμίας $\sim$ στο P ορίζουμε τα σύνολα $\Omega(\sim)$ και $\Omega_{\leq}(\sim)$ ως εξής: $\Omega(\sim) := (\omega \in Z_N^{2n} : \omega_a = \omega_b$ όταν $a \sim b$ και $\omega_a \neq \omega_b$, όταν δεν ισχύει $a \sim b)$ δηλαδή χωρίζει το Z_N^{2n} σε διαφορετικές κλάσεις ανάλογα με ποια σχέση ισοδυναμίας παίρνουμε. Επίσης ορίζουμε $\Omega_{\leq}(\sim) := (\omega \in Z_N^{2n} : \omega_a = \omega_b$ όταν $a \sim b)$ Για παράδειγμα, αν πάρουμε για $n = 2$ και την σχέση ισοδυναμίας όπου $1 \sim 4$ και $2 \sim 3$ τότε θα έχουμε

$$\Omega(\sim) = \left\{\omega \in Z_N^4 : \omega_1 \sim \omega_4, \omega_2 \sim \omega_3 \wedge \neg\omega_1 \sim \omega_2\right\}$$

και

$$\Omega(\sim) = \left\{\omega \in Z_N^4 : \omega_1 \sim \omega_4, \omega_2 \sim \omega_3\right\}.$$

Με βάση τον παραπάνω συμβολισμο και επειδή τα I_n είναι ανεξάρτητα και ακολουθούν την ίδια κατανομή, ο υπολογισμός της $E\left[\prod_{j=1}^{2n} I_{\{\omega_j \in \Omega\}}\right]$ έχει να κάνει μονάχα με την σχέση ισοδυναμίας $\sim_\omega$. Οπότε τελικά θα έχουμε ότι

$$E\left[\prod_{j=1}^{2n} I_{\omega_j \in \Omega}\right] = \tau^{|A/\sim|}$$

όπου $A/\sim$ είναι οι κλάσεις ισοδυναμίας της $\sim$. Άρα η (15) τελικά γίνεται

$$E(Tr(H_0^{2n})) = \sum_{t_1, t_2, \ldots, t_{2n} : t_j \neq t_{j+1}} \sum_{\sim \in P(A)} \tau^{|A/\sim|} \sum_{\omega \in \Omega(\sim)} e^{\frac{2\pi i}{N} \sum_{j=1}^{2n} \omega_j (t_j - t_{j+1})} \tag{16}$$

Όπου το $\sim$ παίρνει τιμές από το $P(A)$, και για κάθε τέτοια σχέση ισοδυναμίας αθροίζουμε τα ω που είναι συμβατα με την $\sim$ και πολλαπλασιάζουμε με την μέση τιμή του I, δηλαδή με τ στην δύναμη $|A/\sim|$. Ο τύπος (16) είναι ο πρώτος τύπος για την αναμενόμενη τιμή του $Tr(H_0^{2n})$. Το πρόβλημα με την παραπάνω έκφραση είναι ότι καθώς παίρνουμε τα $\omega \in \Omega(\sim)$ μας εμφανίζονται κάποια αθροίσματα της μορφής $\sum_{\omega : \omega_i \neq \omega_j}$ που είναι δύσκολο να υπολογίσουμε. Πριν συνεχίσουμε θα δούμε ένα παράδειγμα ώστε να γίνει κατανοητό γιατί ο τύπος (16) δεν είναι τόσο εύχρηστος.

Για παράδειγμα για $n = 1$ έχουμε μόνο δύο σχέσεις ισοδυναμίας στο $\{1, 2\}$, όταν τα ω_1, ω_2 είναι ισοδύναμα μεταξύ τους και όταν τα ω_1, ω_2 δεν είναι. Οπότε το δεξιό μέλος της (16) θα γίνει

$$\sum_{t_1, t_2 : t_1 \neq t_2} \left[\sum_{(\omega_1, \omega_2) \in Z_N^2 : \omega_1 = \omega_2} e^{\frac{2\pi i}{N} \omega_1 (t_1 - t_1)} + \tau^2 \sum_{(\omega_1, \omega_2) \in Z_N^2 : \omega_1 \neq \omega_2} e^{\frac{2\pi i}{N} \omega_1 (t_1 - t_2) + \omega_2 (t_2 - t_1)} \right]$$

Ο στόχος μας είναι να ξαναγράψουμε την έκφραση που είναι μέσα στην αγκύλη με άλλον τρόπο ώστε να μην εμφανίζεται στο άθροισμα το $\omega_1 \neq \omega_2$. Ένας τρόπος να το κάνουμε αυτό είναι να αθροίσουμε για όλα τα $(\omega_1, \omega_2) \in Z_N^2$ και στην συνέχεια να αφαιρέσουμε όλα εκείνα τα στοιχεία που πήραμε στην περίπτωση που $\omega_1 = \omega_2$. Συμβολικά αυτό γράφεται ως εξής

$$\sum_{(\omega_1, \omega_2) \in Z_N^2 : \omega_1 \neq \omega_2} = \sum_{(\omega_1, \omega_2) \in Z_N^2} - \sum_{(\omega_1, \omega_2) \in Z_N^2 : \omega_1 = \omega_2}$$

Στην συνέχεια είναι εύκολο να υπολογίσουμε το $\sum_{(\omega_1,\omega_2)\in Z_N^2}$ καθώς έχουμε ότι

$$\sum_{\omega_1,\omega_2} e^{\frac{2\pi i}{N}\omega_1(t_1-t_2)+\omega_2(t_2-t_1)} = \sum_{\omega_1} e^{\frac{2\pi i}{N}\omega_1(t_1-t_2)} \cdot \sum_{\omega_2} e^{\frac{2\pi i}{N}\omega_2(t_2-t_1)}$$

και κάθε ένα από τα αθροίσματα στο δεξιό μέλος ισούται με 0 ή N ανάλογα με το αν $t_1 = t_2$ ή όχι.

Στην συνέχεια θα γενικεύσουμε αυτές τις ιδέες και θα αναπτύξουμε μια ταυτότητα που θα μας επιτρέψει αν γράψουμε αθροίσματα πάνω από το $\Omega(\sim)$ σε αθροίσματα πάνω από το $\Omega_{\leq}(\sim)$.

Inclusion-Exlusion formula.

Λήμμα 4.1. [7] *(H Inclusion-Exlusion formula για ισοδύναμες κλάσεις.) Έστω A και G δύο μη κενά πεπερασμένα σύνολα. Για κάθε κλάση ισοδυναμίας $\sim\in P(A)$ στο $\omega \in G^{|A|}$, έχουμε ότι*

$$\sum_{\omega\in\Omega(\sim)} f(\omega) = \sum_{\sim_1\in P:\sim_1\leq\sim} (-1)^{|A/\sim|-|A/\sim_1|} \left(\prod_{A'\in A/\sim_1} (|A'/\sim|-1)! \sum_{\omega\in\Omega_{\leq(\sim_1)}} f(\omega) \right). \tag{17}$$

Για να καταλάβουμε τι λέει αυτό το λήμμα ας δούμε το παρακάτω απλό παράδειγμα. Αν $A = \{1,2,3\}$ και $\sim$ είναι η ισότητα, δηλαδή $j \sim k$ αν και μόνο αν $j = k$, τότε η (17) θα γίνει

$$\sum_{\omega_1,\omega_2,\omega_3\in G^n:\omega_1\neq\omega_2\neq\omega_3} f(\omega_1,\omega_2,\omega_3) = \sum_{\omega_1,\omega_2,\omega_3\in G} f(\omega_1,\omega_2,\omega_3) - \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_1=\omega_2} f(\omega_1,\omega_2,\omega_3)$$
$$- \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_2=\omega_3} f(\omega_1,\omega_2,\omega_3) - \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_3=\omega_1} f(\omega_1,\omega_2,\omega_3) + 2 \sum_{\omega_1,\omega_2,\omega_3\in G:\omega_1=\omega_2=\omega_3} f(\omega_1,\omega_2,\omega_3).$$

Οι αριθμοί Stirling.

Όπως προείπαμε ο στόχος μας είναι να γράψουμε την (16) σαν ένα άθροισμα πάνω από το $\Omega_{\leq}(\sim)$. Για να το κάνουμε αυτό εκτός από το παραπάνω λήμμα θα χρειαστούμε άλλο ένα εργαλείο από την συνδυαστική, τους αριθμούς Stirling, οι οποίοι θα μας φανούν πολύ χρήσιμοι στην συνέχεια.

Ο αριθμός Stirling δεύτερου είδους $S(n,k)$ ορίζεται ως εξής. Για κάθε $n,k \geq 0$, $S(n,k)$ είναι ο αριθμός των σχέσεων ισοδυναμίας πάνω από ένα σύνολο με n στοιχεία το οποίο έχει ακριβώς k κλάσεις ισοδυναμίας. Δηλαδή

$$S(n,k) = \#\left\{\sim\in P(A) : |A/\sim| = k\right\}.$$

Έτσι με αυτόν τον ορισμό έχουμε ότι $S(0,0) = S(1,1) = S(2,1) = S(2,2) = 1$ ενώ $S(3,2) = 3$ διότι πάνω από ένα σύνολο με τρεία στοιχεία μπορούμε να βρούμε τρεις σχέσεις ισοδυναμίας ώστε να έχει δύο κλάσεις ισοδυναμίας. Απλά ξεχωρίζουμε κάθε φορά ένα στοιχείο σε σχέση με τα άλλα δύο στις κλάσεις ισοδυναμίας και έχουμε ακριβώς τρεις τρόπους.

Αν τώρα έχουμε ένα στοιχείο a του A και $\sim$ είναι η σχέση ισοδυναμίας στο A με k κλάσεις ισοδυναμίας, τότε το a είτε δεν θα είναι ισοδύναμο με κανένα άλλο στοιχείο και άρα θα έχουμε ότι η σχέση ισοδυναμίας $\sim$ θα έχει ακριβώς $k-1$ κλάσεις ισοδυναμίας στο $A/\{a\}$, είτε θα είναι ισοδύναμο με κάποιο άλλο στοιχείο και άρα θα ανοίκει σε μία από τις k κλάσεις ισοδυναμίας, δηλαδή θα έχουμε k επιλογές. Δηλαδή για κάθε $n,k \geq 0$ έχουμε ότι

$$S(n+1,k) = S(n,k-1) + kS(n,k). \tag{18}$$

Αυτή η σχέση μεταξύ των αριθμών Stirling θα μας φανεί χρήσιμη στην συνέχεια. Παρακάτω θα δούμε μια ταυτότητα για τους αριθμούς Stirling.

Λήμμα 4.2. *Για κάθε $n \geq 1$ και $0 \leq \tau < 1/2$ έχουμε ότι*

$$\sum_{k=1}^{n} (k-1)!S(n,k)(-1)^{n-k}\tau^k = \sum_{k=1}^{\infty} (-1)^{n-k} \frac{\tau^k k^{n-1}}{(1-\tau)^k} \tag{19}$$

Παρατηρείστε ότι η σειρά συγκλίνει επειδή $\tau/(1-\tau) < 1$, αφού $\tau < 1/2$.

Απόδειξη. Θα αποδείξουμε το παραπάνω λήμμα με επαγωγή ως προς n.
Για $n = 1$ έχουμε ότι το αριστερό μέλος της ταυτότητας είναι ίσο με $0!S(1,1)(-1)^0\tau = \tau$, ενώ το δεξί μέλος θα γίνει

$$\sum_{k=1}^{\infty} (-1)^{k+1} \frac{\tau^k}{(1-\tau)^k} = -\sum_{k=0}^{\infty} (\frac{\tau}{\tau-1})^k + 1 = \frac{-1}{1-\frac{\tau}{\tau-1}} + 1 = \tau - 1 + 1 = \tau.$$

Άρα για $n = 1$ ισχύει η ισότητα. Έστω τώρα ότι η παραπάνω ισότητα ισχύει για ένα n με $n \geq 0$. Αν εφαρμόσουμε τον τελεστή $(\tau^2 - \tau)\frac{d}{d\tau}$ στην (19) θα έχουμε ότι το δεξί μέλος γίνεται

$$\begin{aligned}
&(\tau^2-\tau)\frac{d}{d\tau}\sum_{k=1}^{\infty}(-1)^{n+k}\frac{\tau^k k^{n-1}}{(1-\tau)^k} = \\
&= (\tau^2-\tau)\sum_{k=1}^{\infty}(-1)^{n+k}k^{n-1}\frac{k\tau^{k-1}}{(1-\tau)^{k+1}} \\
&= -\tau\sum_{k=1}^{\infty}(-1)^{n+k}k^n\frac{\tau^{k-1}}{(a-\tau^k)} \\
&= \sum_{k=1}^{\infty}(-1)^{n+k+1}\frac{k^n\tau^k}{(1-\tau)^k}.
\end{aligned}$$

Αν τώρα εφαρμόσουμε τον τελεστή στο αριστερό μέλος θα έχουμε ότι

$$\begin{aligned}
&(\tau^2-\tau)\frac{d}{d\tau}\sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}\tau^k = \\
&= \sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}k\tau^{k+1} - \sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}k\tau^k \\
&= \sum_{k=1}^{n}k!S(n,k)(-1)^{n-k}\tau^{k-1} + \sum_{k=1}^{n}k!S(n,k)(-1)^{n-k+1}\tau^k.
\end{aligned}$$

Αλλάζοντας στο πρώτο άθροισμα την μεταβλητή ώστε να ξεκινάει από $k = 2$ και στην συνέχεια επειδή ο όρος που αντιστοιχεί για $k = 1$ είναι μηδέν αφού $S(n,0) = 0$, το άθροισμα θα είναι από $k = 1$ μέχρι $n+1$. Για το δεύτερο άθροισμα το γράφουμε ως άθροισμα από

$k=1$ μέχρι $n+1$ και αφαιρούμε τον όρο που αντιστοιχεί για $k=n+1$ που όμως θα είναι μηδέν επειδή θα εμφανιστεί ο παράγοντας $S(n,n+1)$ που είναι μηδέν. Άρα τελικά θα έχουμε

$$\sum_{k=1}^{n+1}(k-1)!S(n,k-1)(-1)^{n-k+1}\tau^k+\sum_{k=1}^{n+1}k!S(n,k)(-1)^{n-k+1}\tau^k$$

παραγοντοποιώντας και χρησιμοποιώντας την (18) τελικά θα έχουμε ότι

$$\sum_{k=1}^{n+1}(k-1)!(S(n,k-1)+kS(n,k))(-1)^{n-k+1}\tau^k=\sum_{k=1}^{n+1}(k-1)!S(n+1,k)(-1)^{n-k+1}\tau^k$$

και άρα ισχύει για $n+1$, οπότε τελειώσαμε με την απόδειξη του λήμματος. □

Αν τώρα θέσουμε ως $F_n(\tau)$ την ποσότητα (19), δηλαδή

$$F_n(\tau)=\sum_{k=1}^{n}(k-1)!S(n,k)(-1)^{n-k}\tau^k=\sum_{k=1}^{\infty}(-1)^{n-k}\frac{\tau^k k^{n-1}}{(1-\tau)^k} \tag{20}$$

θα έχουμε ότι $F_1(\tau)=\tau$, $F_2(\tau)=-\tau+tau^2$, $F_3(\tau)\tau-3\tau^2+2\tau^3$, $F_4(\tau)=-\tau+7\tau^2-32\tau^3+6\tau^4$ και τα λοιπά. Στην συνέχεια θα θέλαμε να βρούμε ένα φράγμα για την F_n. Το παρακάτω λήμμα μας δείνει ένα καλό φράγμα.

Λήμμα 4.3. *Έστω $n\neq 1$ και $0\leq\tau<1/2$. Αν $\frac{\tau}{1-\tau}\leq e^{1-n}$, τότε έχουμε ότι*

$$|F_n(\tau)|\leq\frac{\tau}{1-\tau}.$$

Αν αντιθέτως $\frac{\tau}{1-\tau}>e^{1-n}$, τότε έχουμε ότι

$$|F_n(\tau)|\leq e^{\left[(n-1)(\log(n-1)-\log\log\frac{1-\tau}{\tau}-1)\right]}.$$

Απόδειξη. Αν πάρουμε για $g(x)=\frac{\tau^x x^{n-1}}{(1-\tau)^x}$, τότε από στοιχειώδη απειροστικό λογισμό θα έχουμε ότι η g παρουσιάζει ολικό μέγιστο στο $x_0=(n-1)/\log\frac{1-\tau}{\tau}$. Οπότε, αν $\frac{\tau}{1-\tau}\leq e^{1-n}$ θα έχουμε ότι $x_0\leq\frac{n-1}{n-1}=1$. Οπότε και για την εναλλάσσουσα σειρά $F_n(\tau)=\sum_{k=1}^{\infty}(-1)^{n+k}g(k)$ θα έχουμε ότι είναι το πολύ $g(1)=\frac{\tau}{1-\tau}$.
Διαφορετικά, αν δηλαδή $\frac{\tau}{1-\tau}\geq e^{1-n}$, τότε έχουμε ότι $x_0=\frac{n-1}{\log(\frac{1-\tau}{\tau})}<1$ με $g(x_0)=e^{\left[(n-1)(\log(n-1)-\log\log\frac{1-\tau}{\tau}-1)\right]}$ και η σειρά -όπως πριν- είναι φραγμένη από το $g(x_0)$. □

Θα μας φανεί χρήσιμο για την συνέχεια να γράψουμε το φράγμα της F_n ως εξής.

$$F_n(\tau)\leq G(n) \tag{21}$$

όπου $G(n)=\frac{\tau}{1-\tau}$ για $\log\frac{\tau}{1-\tau}\leq 1-n$ και
$G(n)=e^{\left[(n-1)(\log(n-1)-\log\log\frac{1-\tau}{\tau}-1)\right]}$ για $\log\frac{\tau}{1-\tau}>1-n$.
Παρατηρείστε ότι γράψαμε την G σαν συνάρτηση του n και όχι του τ διότι έτσι θα μας χρησιμεύσει στην συνέχεια. Με βάση όλα τα παραπάνω, τώρα είμαστε έτοιμοι να δώσουμε έναν δεύτερο τύπο για την αναμενόμενη τιμή $E[TrH_0^{2n}]$.

Ο δεύτερος τύπος για την μέση τιμή του $Tr(H_0^{2n})$.

Ας ξαναθυμηθούμε την (17), η οποία είναι η εξής

$$E(Tr(H_0^{2n})) = \sum_{t_1,t_2,\ldots,t_{2n}:t_j\neq t_{j+1}} \sum_{\sim\in P(A)} \tau^{|A/\sim|} \sum_{\omega\in\Omega(\sim)} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j-t_{j+1})}.$$

Το εσωτερικό άθροισμα της (17) μπορούμε να το γράψουμε ως

$$\sum_{\sim\in P(A)} \tau^{|A/\sim|} \sum_{\omega\Omega(\sim)} f(\omega)$$

με $f(\omega) = e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j-t_{j+1})}$. Παρακάτω θα αποδείξουμε μια ταυτότητα που εμπλέκει αθροίσματα αυτής της μορφής.

Λήμμα 4.4. *Ισχύει η παρακάτω ισότητα*

$$\sum_{\sim\in P(A)} \tau^{|A/\sim|} \sum_{\omega\in\Omega(\sim)} f(\omega) = \sum_{\sim_1\in P(A)} \left[\sum_{\omega\in\Omega_{\leq}(\sim_1)} f(\omega)\right] \prod_{A'\in A/\sim_1} F_{|A'|}(\tau).$$

Απόδειξη. Εφαρμόζοντας την (17) στο αριστερό μέλος και αναδιατάσσοντας θα έχουμε

$$\sum_{\sim_1\in P(A)} T(\sim_1) \sum_{\omega\in\Omega_{\leq(\sim_1)}} f(\omega)$$

όπου

$$T(\sim_1) = \sum_{\sim\in P(A):\sim\geq\sim_1} \tau^{|A/\sim|}(-1)^{|A/\sim|-|A/\sim_1|} \prod_{A'\in A/\sim_1} (|A'/\sim|-1)!.$$

Διαχωρίζοντας τώρα το A στις κλάσεις ισοδυναμίας A' ως προς την σχέση $\sim_1$, δηλαδή τις κλάσεις A' του $A/\sim_1$ θα έχουμε

$$T(\sim_1) = \prod_{A'\in A/\sim_1} \sum_{\sim'\in P(A')} \tau^{|A'/\sim'|}(-1)^{|A'/\sim'|-|A'|}(|A'/\sim'|-1)!.$$

Ουσιαστικά αυτό που κάναμε ήταν να εναλλάξουμε το άθροισμα με το γινόμενο παίρνοντας πρώτα το γινόμενο από τις κλάσεις A' του $A/\sim_1$ και στην συνέχεια το άθροισμα. Παρατηρείστε ότι σε αυτήν την περίπτωση για κάθε σχέση $\sim'\in P(A')$ έχουμε ότι $\sim'\geq\sim_1$ καθώς επίσης και ότι ο δεύτερος όρος του εκθέτη του (-1) είναι $|A'/\sim_1|$ που είναι $|A'|$ οπότε τελικά μπορούμε να κάνουμε αυτήν την εναλλαγή.

Διαχωρίζοντας τώρα την $\sim'$ με βάση τον αριθμό των ισοδύναμων κλάσσεων $|A'/\sim'|$ θα έχουμε

$$\prod_{A'\in A/\sim_1} \sum_{k=1}^{|A'|} S(|A'|,k)\tau^k(-1)^{k-|A'|(k-1)!}$$

Όπου το k είναι το πλήθος των κλάσεων, δηλαδή $k=|A'/\sim'|$ και $S(|A'|,k)$ είναι όπως γνωρίζουμε το πλήθος των ισοδύναμων κλάσεων του A' που έχουν ακριβώς $|A'/\sim'|$ κλάσσεις ισοδυναμίας. Οπότε πολλαπλασιάζοντας με $S(|A'|,k)$ δεν έχουμε χάσει καμμία σχέση και διατηρείται η ισότητα. Τέλος από την (20) θα έχουμε το ζητούμενο, δηλαδή

$$T(\sim_1) = \prod_{A'\in A/\sim_1} \sum_{k=1}^{|A'|} S(|A'|,k)\tau^k(-1)^{k-|A'|(k-1)!} = \prod_{A'\in A/\sim_1} F_{|A'|}(\tau)$$

και άρα

$$\sum_{\sim\in P(A)} \tau^{|A/\sim|} \sum_{\omega\in\Omega(\sim)} f(\omega) = \sum_{\sim_1\in P(A)} \left[\sum_{\omega\in\Omega_{\leq}(\sim_1)} f(\omega) \right] \prod_{A'\in A/\sim_1} F_{|A'|}(\tau).$$

□

Εφαρμόζοντας τώρα το παραπάνω λήμμα, Λήμμα 4.4, στην (17) έχουμε ότι

$$E[Tr(H_0^{2n})] = \sum_{\sim\in P(A)} \sum_{t_1,\ldots,t_{2n}\in T: t_j\neq t_{j+1}} \sum_{\omega\in\Omega_{\leq(\sim)}} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j-t_{j+1})} \prod_{A'\in A/\sim} F_{|A'|}(\tau). \tag{22}$$

Στην συνέχεια θα υπολογίσουμε το

$$I(\sim) = \sum_{\omega\in\Omega_{\leq(\sim)}} e^{\frac{2\pi i}{N}\sum_{j=1}^{2n}\omega_j(t_j-t_{j+1})}$$

αλλά πρώτα θα απλοποιήσουμε τον συμβολισμό. Για κάθε κλάση $A' \in A/\sim$ ορίζουμε $t_{A'} = \sum_{a\in A'}(t_a - t_{a+1})$, και $\omega_{A'} = \omega_a$ για κάθε $a \in A'$ (όλα αυτά τα a είναι ισοδύναμα αφού έχουμε ότι $\omega \in \Omega_{\leq}(\sim)$ και άρα $\omega_b = \omega_c$ όταν τα b και c είναι ισοδύναμα). Τότε θα έχουμε

$$I(\sim) = \sum_{(\omega_{A'})_{A'\in A/\sim}\in Z_N^{|A/\sim|}} e^{\frac{2\pi i}{N}\sum_{A'\in A/\sim}\omega_{A'}t_{A'}} = \prod_{A'\in A/\sim}\sum_{\omega_{A'}\in Z_N} e^{\frac{2\pi i}{N}\omega_{A'}t_{A'}}$$

κάνοντας το άθροισμα στο εκθετικό γινόμενο. Παρατηρείστε ότι το άθροισμα είτε είναι ίσο με $|Z_N| = N$, ότα $t_{A'} = 0$, είτε ίσο με μηδέν διαφορετικά. Έτσι στην ουσία έχουμε αποδείξει το παρακάτω λήμμα.

Λήμμα 4.5. *Για κάθε κλάση $A' \in A/\sim$, ορίζουμε $t_{A'} := \sum_{a\in A'}(t_a - t_{a+1})$. Τότε*

$$E[Tr(H_0^{2n})] = \sum_{\sim\in P(A)} \sum_{t\in T^{2n}: t_j\neq t_{j+1}\wedge\forall A' t_{A'}=0} N^{|A/\sim|} \prod_{A'\in A/\sim} F_{|A'|}(\tau) \tag{23}$$

Αυτός ο τύπος θα αποτελέσει το βασικό εργαλείο μας για τις εκτιμήσεις που θα κάνουμε κατά την απόδειξη του θεωρήματος (3.1). Και αυτό επειδή στο δεύτερο άθροισμα το $t_j \neq t_{j+1}$ μας εξασφαλίζει ότι αν το $A/\sim$ περιέχει κάποια κλάση ισοδυναμίας που να είναι μονοσύνολο τότε το άθροισμα θα ισούτε με μηδέν.

Η απόδειξη του θεωρήματος 3.1.

Έστω $\sim$ μια ισοδυναμία όπου καμία από τις κλάσεις ισοδυναμίας της δεν είναι μονοσύνολο. Τότε θα έχουμε ότι

$$\#\left\{t \in T^{2n} : t_{A'} = 0 \forall A' \in A/\sim\right\} \leq |T|^{2n-|A/\sim|+1}$$

Διότι αν δούμε τα $t_j - t_{j+1}$ σαν γραμμικό συνδυασμό των $t_1, ..., t_{2n}$, τότε είναι γραμμικώς ανεξάρτητα εκτός από το $\sum_{j=1}^{2n} t_j - t_{j+1}$ που κάνει μηδέν. Οπότε θα έχουμε $|A/\sim| - 1$ ανεξάρτητους όρους στο παραπάνω άθροισμα και άρα το πλήθος των διαφορετικών t που είναι στο παραπάνω άθροισμα είναι το πολύ $|T|^{2n-|A/\sim|+1}$. Οπότε χρησημοποιώντας το παραπάνω φράγμα και την (21) στην (23) τελικά θα έχουμε ότι

$$E[Tr(H_0^{2n})] \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} \sum_{\sim\in P(A,k)} \prod_{A'\in A/\sim} G(|A'|)$$

όπου το $P(A,k)$ δηλώνει όλες τις σχέσεις στο A με k κλάσεις εκ των οποίων καμία δεν είναι μονοσύνολο. Η παραπάνω ανισότητα προκύπτει διότι το k είναι το πλήθος των κλάσεων μιας

ισοδυναμίας, δηλαδή $k = |A'/\sim|$ οπότε ο δείκτης του δεύτερου αθροίσαμτος $\sim \in P(A,k)$ μας εξασφαλίζει ότι για κάθε σχέση παίρνουμε όλες τις κλάσεις χωρίς τα μονοσύνολα, όπως ακριβώς και πριν, μόνο που πρέπει να πολλαπλασιάσουμε με $|T|^{2n-|A/\sim|+1}$. Η αλλαγή που κάναμε στο γινόμενο οφείλεται στην ανισότητα (21).

Τον παραπάνω τύπο για την αναμενόμενη τιμη θα τον γράψουμε ως εξης

$$E[Tr(H_0^{2n})] \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} Q(n,k) \tag{24}$$

όπου

$$Q(n,k) = \sum_{\sim \in P(A,k)} \prod_{A' \in A/\sim} G(|A'|)$$

και θα βρούμε κατάλληλο φράγμα για την ποσότητα $Q(n,k)$. Πριν από αυτό θα δώσουμε έναν τύπο για την G που θα μας χρησιμεύσει στην συνέχεια. Για $\tau \leq 1/(1+e)$ έχουμε

$$G(n+1) \leq nG(n) \tag{25}$$

για κάθε $n \geq 1$. Για να δούμε ότι ισχύει ο παραπάνω τύπος αρκει να δούμε ότι η G είναι κυρτή οπότε

$$\log G(n+1) \leq \log G(n) + \frac{d}{dn} \log G(n+1)$$

και στη συνέχεια αρκει να δούμε ότι $\frac{d}{dn} \log G(n+1) \leq \log n$ όταν $\log(\log \frac{1-\tau}{\tau}) \geq 1$.

Τώρα, το φράγμα που μας βολεύει για την $Q(n,k)$ είναι το εξής: Για κάθε $n \geq 2$, $k \geq 1$ έχουμε

$$Q(n,k) \leq (n-1)Q(n-1,k) + (n-1)G(2)Q(n-2,k-1) \tag{26}$$

το οποίο προκύπτει ως εξής. Έστω ότι το a είναι ένα στοιχείο του A και $\sim$ μια σχέση ισοδυναμίας στο $P(A,k)$. Τότε θα έχουμε δύο επιλογές. Πρώτων, το a θα ανήκει σε μια κλάση ισοδυναμίας, την A', η οποία έχει ένα ακόμα στοιχείο, το b και έχουμε ακριβώς $n-1$ επιλογές για το b αφού έχουμε συνολικά n στοιχεία. Άρα παίρνοντας την A' εμφανίζεται ο όρος $(n-1)G(2)Q(n-2,k-1)$ καθώς έχουμε $n-1$ επιλογές για το b, $|A'/\sim| = 2$ οπότε $G(|A'/\sim|) = G(2)$ και τέλος αφού βγάλουμε την κλάση A' θα έχουμε $n-2$ στοιχεία σε $k-1$ κλάσεις ισοδυναμίας άρα γιαυτό έχουμε το $Q(n-2,k-1)$. Για την δεύτερη επιλογή έχουμε ότι το a θα ανήκει σε μια κλάση ισοδυναμίας με περισσότερα από δύο στοιχεία, οπότε αν πάρουμε το a από το A θα δημιουργήσουμε μια κλάση ισοδυναμίας στο $P(A/\{a\},k)$. Έστω τώρα $\sim'$ να είναι μια σχέση ισοδυναμίας από το $P(A/\{a\},k)$ και έστω A_1,A_2...A_k οι αντίστοιχες κλάσεις της $\sim'$. Αν βάλουμε το στοιχείο a σε μια από αυτές τις κλάσεις, έστω στην A_i τότε, σύμφωνα με τον παραπάνω τύπο για την G, (25), το $G(|A_i|)$ θα αυξηθεί το πολύ κατά $|A_i|$. Οπότε για αυτήν την περίπτωση η Q θα είναι μικρότερη από

$$\sum_{\sim' \in P(A/\{a\},k)} \sum_{i=1}^{k} |A_i| \prod_{A' \in A/\sim} G(|A'|).$$

Όμως $\sum_{i=1}^{k} |A_i| = n-1$ αφού $|A/\{a\}| = n-1$ οπότε τελικά η παραπάνω έκφραση θα γίνει

$$(n-1) \cdot \sum_{\sim' \in P(A/\{a\},k)} \prod_{A' \in A/\sim} G(|A'|) = (n-1)Q(n-1,k)$$

και άρα έτσι προκύπτει η ανισότητα για το $Q(n,k)$.

Τώρα με επαγωγή και με την βοήθεια της (26) θα δείξουμε ότι

$$Q(n,k) \leq G(2)^k (2n)^{n-k} \tag{27}$$

Η ανισότητα ισχύει για $Q(1,k)$. Έστω τώρα ότι ισχύει για όλα τα (m,k), με $m < n$. Από την (26) έχουμε ότι

$$Q(n,k) \leq (n-1)Q(n-1,k) + (n-1)G(2)Q(n-2,k-1)$$

και χρησιμοποιώντας την επαγωγική υπόθεση, παραγοντοποιώντας και απλοποιώντας και κάνοντας τετριμμένες εκτιμήσεις θα έχουμε ότι

$$Q(n,k) \leq G(2)^k \left(2^{n-k-1}(n-1)^{n-k-1} + 2^{n-k-2}(n-1)^{n-k-1}\right) \leq G(2)^k (2n)^{n-k}.$$

Στην συνέχεια, με βάση το φράγμα για το $Q(n,k)$ που μας δείνει η (27) (ουσιαστικά χρησιμοποιούμε μια πιο χονδροειδή εκτίμηση) για την αναμενόμενη τιμή, θα έχουμε

$$E[Tr(H_0^{2n})] \leq \sum_{k=1}^{n} N^k |T|^{2n-k+1} G(2)^k (4n)^{2n-k}$$

Αν θέσουμε με b όλους τους παράγοντες που έχουν στον εκθέτη τους το k, δηλαδη $b = NG(2)/(4n|T|)$, τότε το δεξιό μέλος θα γίνει

$$|T|^{2n+1}(4n)^{2n} \sum_{k=1}^{n} b^k$$

και αφού το $n \cdot max(b, b^n)$ είναι ένα φράγμα για το άθροισμα, τελικα για την αναμενομενη τιμή θα έχουμε ότι

$$E[Tr(H_0^{2n})] \leq nN^n |T|^{n+1} G(2)^n (4n)^n$$

όταν $n \leq NG(2)/4|T|$, δηλαδή όταν $b \geq 1$ και άρα $max(b, b^n) = b^n$, ενώ διαφορετικά θα έχουμε

$$E[Tr(H_0^{2n})] \leq nN|T|^{2n} G(2)(4n)^{2n-1}$$

Επειδή $G(2) = \tau/(1-\tau)$ έχουμε σχεδον τελειώσει με την αποδειξη του θεωρήματος. Το μόνο προβλημα που έχουμε είναι ότι όταν το n είναι μικρο (πρώτη ανισοτητα) μας λείπει ο παράγοντας e^{-n} και είναι το μόνο πλέον που μένει να διορθώσουμε για να ολοκληρώσουμε την απόδειξη του θεωρήματος 3.3.

Για να διορθώσουμε αυτό το πρόβλημα, θα χρειαστούμε μια καλύτερη προσέγγιση. Αν βάλουμε στην (24) $n = 2k$ θα έχουμε

$$Q(2k,k) \leq (2k-1)Q(2k-1,k) + (2k-1)G(2)Q(2k-2,k-1) = (2k-1)G(2)Q(2k-2,k-1)$$

αφού $Q(n,k) = o$ για $n < 2k$ οπότε συνεχίζοντας επαγωγικά, θα έχουμε ότι

$$Q(2k,k) \leq (2k-1)(2k-3)G(2)^2 Q(2(k-2),k-1)$$

και τελικά

$$Q(2k,k) \leq (2k-1)(2k-3)...3G(2)^k = \frac{(2k-1)!}{2^{k-1}(k-1)!} G(2)^k$$

Για να δουμε ότι ισχύει η τελευταία ισότητα αρκεί να παρατηρήσουμε ότι στο αριστερό μέλος έχουμε όλους τους περιττούς όρους του $(2k-1)!$ ενώ στον παρανομαστή του δεξιού μέλους αν πολλαπλασιάσουμε κάθε παράγοντα του παραγοντικού με 2 θα πάρουμε όλους τους άρτιους. Στην συνέχεια πάλι με επαγωγή μπορούμε να δείξουμε ότι

$$Q(n,k) \leq (n-1)(n-2)...2k2^{n-k} Q(2k,k) = \frac{(n-1)!}{(k-1)!} 2^{n-2k+1} G(2)^k$$

που είναι καλύτερη εκτίμηση από την (27). Οπότε χρησιμοποιώντας το παραπάνω στην (24) θα έχουμε ότι

$$E[Tr(H_0^{2n})] \leq \sum_{k=1}^{n} B(2n,k)$$

όπου

$$B(2n,k) = \frac{(2n-1)!}{(k-1)!} N^k |T|^{2n-k+1} 2^{2n-2k+1} G(2)^k.$$

Τώρα, με απλούς υπολογισμούς μπορούμε να δούμε ότι

$$\frac{B(2n,k)}{B(2n,k-1)} = \frac{NG(2)}{4|T|(k-1)}.$$

Παρατηρήστε, ότι για σταθερό n με $n \leq NG(2)/(4|T|)$ ότι η $B(2n,k)$ είναι αύξουσα ως προς k οπότε θα έχουμε ότι

$$\sum_{k=1}^{n} B(2n,k) \leq nB(2n,n)$$

και άρα η εκτίμηση θα γίνει

$$E[Tr(H_0^{2n})] \leq nB(2n,n) = n\frac{(2n)!}{n!} G(2)^n |T|^{n+1} N^n. \tag{28}$$

Για να απλοποιήσουμε το κλάσμα $(2n)!/n!$ θα χρησιμοποιήσουμε την παρακάτω προσέγγιση Stirling

$$\sqrt{2\pi} n^{n+1/2} e^{-n+1/(12n+1)} < n! < \sqrt{2\pi} n^{n+1/2} e^{-n+1/12n}.$$

Όπότε κάνοντας τις απλοποιήσεις, για το κλάσμα θα έχουμε ότι

$$\frac{(2n)!}{n!} \leq 2^{2n+1} n^n e^{-n}.$$

Τέλος, κάνοντας την αντικατάσταση στην (28) θα έχουμε ότι

$$E[Tr(H_0^{2n})] \leq 2nN^n |T|^{n+1} G(2)^n (4n)^n e^{-n}$$

και άρα τελειώσαμε με την απόδειξη του θεωρήματος 3.3 καθώς θυμίζουμε ότι $G(2) = \tau/(1-\tau)$. Δηλαδή δείξαμε ότι για $n \leq \frac{\tau N}{4(a-\tau)|T|}$ έχουμε ότι

$$E[Tr(H_0^{2n})] \leq 2\left(\frac{4}{e(1-\tau)}\right)^n n^{n+1} |\tau N|^n |T|^{n+1}$$

που ήταν και το ζητούμενο στο τελευταίο κομμάτι της απόδειξης του θεωρήματος 3.3.

ΚΕΦΑΛΑΙΟ 5

Σχόλια.

ΚΕΦΑΛΑΙΟ 6

Αναφορές.

[1] Terence Tao, An uncertainty principle for cyclyc groups of prime order.

[2] Bao Luong, Fourier analysis on finite abelian groups.

[3] Audrey Terras, Fourier analysis on Finite groups and applications.

[4] Terence Tao, Emmanuel Candes, Justin Romberg, Robust Uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, 2.3 The Bernoulli model, σελ. 15-16.

[5] Noga Alon, Joel H. Spencer, Appendix a bounding of large deviations.

[6] Terence Tao, Emmanuel Candes, Justin Romberg, Robust Uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, 7.2 Proof of Lemma 3.4, σελ. 37-39.

[7] Terence Tao, Emmanuel Candes, Justin Romberg, Robust Uncertainty principles: Exact signal reconstruction from highly incomplete frequency information, 4.2 Iclusion-Exclusion formulae, σελ. 25-26.