Πιθανά θέματα για μεταπτυχιακή εργασία

Μιχάλης Κολουντζάκης

Αύγουστος 2005

Περιεχόμενα

1 Εισαγωγικά

Τα παρακάτω είναι ενδεικτικά θέματα για μεταπτυχιακή εργασία για όποιον ενδιαφέρεται να την εκπονήσει μαζί μου. Τα θέματα είναι ενδεικτικά των ενδιαφερόντων μου και έχουν επίσης επιλεγεί με το κριτήριο να είναι σχετικά σύγχρονα, πέρα από το να έχουν όμορφα μαθηματικά.

Πρόκειται για μια συλλογή θεμάτων από τις περιοχές

1. Αρμονική ανάλυση

2. Θεωρία Αριθμών, Συνδυαστική, Γεωμετρία

3. Θεωρητική Επιστήμη Υπολογιστών

Δεν πρόκειται για αποκλειστική λίστα αλλά περισσότερο για μια λίστα από θέματα και κάποια σχετική βιβλιογραφία που θα επιτρέψει στο φοιτητή να μπορέσει μόνος του να πάρει μια ιδέα για κάποιες περιοχές των Μαθηματικών που ενδιαφέρουν εμένα.

2 Αρμονική ανάλυση

2.1 Ακύρωση (cancellation) γραμμικών μορφών και εφαρμογές

Έστω $n \times n$ πίνακας A που τα στοιχεία του ικανοποιούν τη συνθήκη $|a_{ij}| \leq 1$. Αν το διάνυσμα $x \in \mathbb{R}^n$ υπόκειται στη συνθήκη $x_i = \pm 1$, πόσο 'μικρό' μπορεί να είναι το διάνυσμα Ax; Για να είμαστε πιο σαφείς πόσο μικρή μπορεί να είναι η ℓ^∞ νόρμα του (πόσο μικρό μπορεί να είναι το μεγαλύτερο στοιχείο του);

Η απάντηση είναι [30, 2] ότι υπάρχει σταθερά C τέτοια ώστε μπορεί κανείς να διαλέξει τα πρόσημα x_i ώστε $\|Ax\|_\infty \leq C\sqrt{n}$.

Το πρόβλημα μπορεί να πάρει διάφορες μορφές ανάλογα με τις συνθήκες που επιβάλλονται στον πίνακα A και τη νόρμα στην οποία μετράμε το μέγεθος του Ax. Οι εφαρμογές του είναι πάρα πολλές.

2.2 Σχεδόν σταθερά (ultraflat) πολυώνυμα

Έστω τριγωνομετρικό πολυώνυμο

$$f(x) = \sum_{j=0}^{n-1} a_j e^{2\pi i j x}.$$

Αυτή είναι μια συνεχής, περιδική συνάρτηση με περίοδο 1 της οποίας η L^2 νόρμα είναι η $\sqrt{\sum_{j=0}^{n-1} |a_j|^2}$. Επίσης έχουμε $\|f\|_\infty \geq \|f\|_{L^2}$.

Με τηνεπιπλέον προϋπόθεση ότι οι μιγαδικοί αριθμοί a_j έχουν όλοι μέτρο 1 έχουμε $\|f\|_\infty \geq \|f\|_{L^2} = \sqrt{n}$. Πόσο μικρή μπορεί κανείς να έχει την $\|f\|_\infty$ με κατάλληλη επιλογή των a_j; Ο Kahane [16] απέδειξε ότι μπορεί κανείς για κάθε $\epsilon > 0$ να επιλέξει τα a_j με τρόπο ώστε να έχει $\|f\|_\infty \leq (1+\epsilon)\sqrt{n}$, για αρκετά μεγάλο n. Η μέθοδος είναι πιθανοθεωρητική και ιδιαίτερα ενδιαφέρουσα. Υπάρχουν επίσης αρκετές παραλλαγές του προβλήματος, για παράδειγμα αυτή [20] στην οποία $a_j = \pm 1$ και στην οποία περίπτωση η απάντηση δεν είναι γνωστή.

2.3 Η εικασία του Littlewood για την L^1 νόρμα πολωνύμων

Η εικασία του Littlewood ήταν ότι ένα πολυώνυμο της μορφής

$$p(x) = \sum_{j=1}^{n} c_j e^{2\pi i k_j x},$$

όπου $|c_j| \geq 1$ και $0 \leq k_1 < k_2 < \cdots < k_n$ είναι φυσικοί αριθμοί, έχει αναγκαστικά μεγάλη L^1 νόρμα, και, ειδικότερα, υπάρχει απόλυτη σταθερά $C > 0$ ώστε πάντα να έχουμε $\|p\|_{L^1} \geq C \log n$.

Η εικασία αυτή αποδείχτηκε τελικά το 1980 ανεξάρτητα από τους McGehee, Pigno και Smith [22] και τον Konyagin [19], μετά από μια μακρά σειρά ολοένα και καλύτερων κάτω φραγμάτων που οφειλόταν στους P. Cohen, Davenport, Pichorides και άλλους.

2.4 Αριθμητικές πρόοδοι σε πυκνά σύνολα

Ένα πολύ σημαντικό θεώρημα στη θεωρία Ramsey είναι το θεώρημα του Szemeredi [32]. Αυτό λέει ότι σε κάθε σύνολο φυσικών αριθμών με θετική πυκνότητα μπορούμε να βρούμε αριθμητικές προόδους οποιουδήποτε πεπερασμένου μήκους.

Η αρχική απόδειξη του Szemeredi ήταν στοιχειώδης και φοβερά δύσκολη. Έχει έκτοτε ξαναναποδειχθεί το θεώρημα αυτό είτε με μεθόδους δυναμικών συστημάτων [11] είτε με μεθόδους αρμονικής ανάλυσης [12].

2.5 Ανισοκατανομή (Irregularities of distribution)

Αν έχουμε ένα σύνολο σημείων $X = \{x_1, \ldots, x_n\} \subseteq [0,1]^2$ πόσο ομοιόμορφα κατανεμημένο μπορεί να είναι αυτό; Ένα μέτρο της ομοιομορφίας είναι, παραδείγματος χάρη, το μέγιστο της ποσότητας

$$\frac{|X \cap Q|}{|Q|}$$

όταν Q είναι οποιοδήποτε ορθογώνιο παραλληλόγραμο στο επίπεδο με τις πλευρές του παράλληλες προς τους άξονες.

Προκύπτει ότι όποιο και να είναι το σύνολο σημείων X υπάρχουν κάτω φράγματα γι' αυτή την ποσότητα που πάνε στο άπειρο με το n. Το πόσα μεγάλα είναι αυτά τα φράγματα είναι το αντικείμενο της μελέτης της θεωρίας της *ανισοκατανομής* (irregularity of distribution) και τα προβλήματα που μελετούνται μπορεί να είναι παρόμοιας αλλά και αρκετά διαφορετικής φύσης.

Τα εργαλεία που χρησιμοποιούνται είναι πολύ ενδιαφέροντα και περιλαμβάνουν το μετασχηματισμό Fourier και συνδυαστικές μεθόδους. Κύριες αναφορές είναι τα βιβλία [3, 21, 6].

3 Θεωρία Αριθμών, Συνδυαστική, Γεωμετρία

3.1 Σύνολα με διαφορετικά αθροίσματα, προσθετικές βάσεις ακεραίων

Αν ένα σύνολο $A \subseteq \{1, \ldots, n\}$ έχει την ιδιότητα ότι όλα τα αθροίσματά των στοιχείων του ανά δύο είναι διαφορετικά (τέτοια σύνολα ονομάζονται σύνολα τύπου B_2 ή και σύνολα Sidon), αν δηλ. $a + b = c + d$ και $a, b, c, d \in A$ συνεπάγεται $\{a, b\} = \{c, d\}$, πόσο μεγάλο μπορεί να είναι το σύνολο A; Είναι τώρα γνωστό ότι το μέγεθος $|A|$ μπορεί να είναι τόσο μεγάλο όσο $\sqrt{n} + o(\sqrt{n})$ αλλά όχι $(1+\epsilon)\sqrt{n}$ για οποιοδήποτε $\epsilon > 0$.

Και το άνω αλλά και το κάτω φράγμα παρουσιάζουν μεγάλο ενδιαφέρον, κυρίως στην περίπτωση που το πρόβλημα έχει κάπως παραλλαγεί (τι γίνεται π.χ. αν πάρουμε αθροίσματα ανά τρία δεν είναι τόσο καλά γνωστό) και οι μέθοδοι είναι συνδυαστικές, αναλυτικές ή αλγεβρικές. Η κλασική αναφορά είναι το βιβλίο [14].

Άλλο παρόμοιο πρόβλημα σε αυτό τον κλάδο συνδυαστικής και προσθετικής θεωρίας αριθμών, όπως λέγεται, είναι το εξής. Ας υποθέσουμε ότι το σύνολο $B \subseteq \mathbb{N}$ έχει την ιδιότητα ότι, τελικά, κάθε φυσικός αριθμός γράφεται σαν άθροισμα δύο στοιχείων του B (π.χ., πάρτε B να είναι ο αριθμός 1 και όλοι οι άρτιοι φυσικοί). Ένα τέτοιο σύνολο λέγεται *προσθετική βάση*. Αν συμβολίσουμε με

$$r_B(n) = |\{x, y \in B : \ x \leq y, \ x + y = n\}|$$

το πλήθος τέτοιων αναπαραστάσεων του αριθμού n, τότε πόσο μεγάλη πρέπει να είναι η συνάρτηση $r_B(n)$; Γνωρίζουμε ότι δε χρειάζεται να είναι μεγαλύτερη από $C \log n$ [8] αλλά, αν και έχει εικαστεί από τον Erdős, κανείς δεν έχει δείξει ότι η συνάρτηση αυτή δε μπορεί να είναι φραγμένη.

3.2 Το θεώρημα Erdős-Fuchs

Έστω $B \subseteq \mathbb{N}$ ένα υποσύνολο των φυσικών, και ας συμβολίσουμε, όπως και στην §3.1, με

$$r_B(n) = |\{x, y \in B : \ x \leq y, \ x + y = n\}|$$

το πλήθος των αναπαραστάσεων του φυσικού αριθμού n ως άθροισμα δύο στοιχείων του B. Το θεώρημα Erdős–Fuchs (δείτε, π.χ., [24, 14]) λέει ότι η συνάρτηση αυτή δε μπορεί να συμπεριφέρεται πολύ ομαλά. Ακριβέστερα, αν $R_A(n) = \sum_{j=1}^{n} r_A(j)$ τότε δε μπορεί να ισχύει, όταν $n \to]infty$ η ασυμπτωτική εκτίμηση

$$R_A(n) = Cn + o(n^{1/4}(\log n)^{-1/2}).$$

Η μέθοδος κάνει χρήση μιγαδικής ανάλυσης, κατά τρόπο ο οποίος συναντάται συχνά σε εκτιμήσεις συνδυαστικών ποσοτήτων, με κατάλληλη δηλ. επικαμπύλια ολοκλήρωση και χρήση του θεωρήματος του Cauchy.

3.3 Διαφορετικές αποστάσεις από n σημεία στο επίπεδο

Αν $X = \{x_1, \ldots, x_n\}$ είναι ένα σύνολο από n διαφορετικά σημεία στο επίπεδο πόσες διαφορετικές αποστάσεις, τουλάχιστον, πρέπει αναγκαστικά αυτά να ορίζουν μεταξύ τους;

Το πρόβλημα τέθηκε από τον Erdős [9] (δείτε επίσης το βιβλίο [25]). Αν ονομάσουμε $G(n)$ το ελάχιστο πλήθος διαφορετικών αποστάσεων που ορίζουν τα σημεία ενός οποιουδήποτε συνόλου X με n σημεία, η εικασία που διατύπωσε ο Erdős είναι ότι $G(n) \geq Cn/\log n$. Αν X επιλέξουμε να είναι το σύνολο των σημείων πάνω σε ένα $\sqrt{n} \times \sqrt{n}$ ορθογώνιο πλέγμα, τότε το πλήθος των διαφορετικών αποστάσεων που αυτά ορίζουν έχει αυτή ακριβώς την τάξη μεγέθους.

Από τότε έχουν δοθεί ολοένα και κλύτερα (μεγαλύτερα) κάτω φράγματα για την ποσότητα $G(n)$. Ένα από τα τελευταία (αν και όχι το καλύτερο ως τώρα) είναι ένα αποτέλεσμα του Székely [31] που λέει ότι $G(n) \geq Cn^{4/5}$.

3.4 Προβλήματα απαρίθμησης ως μοντέλα για στατιστική μηχανική

Υπάρχουν πεπερασμένα διακριτά μοντέλα για φαινόμενα στατιστικής μηχανικής που έχουν να κάνουν με απαρίθμηση τρόπων με τους οποίων μπορεί να διαμεριστεί ένα χωρίο σε μη αλληλοεπικαλυπτόμενα αντίγραφα ενός απλού σχήματος. Για παράδειγμα, οι Kasteleyn [17] και Temperley-Fisher [33] υπολόγισαν ακριβώς τον αριθμό διαμερίσεων μιας $m \times n$ σκακιέρας σε ντόμινα, όπου ως ντόμινο θεωρούμε δύο τετράγωνα της σκακιέρας που έχουν μια κοινή ακμή. Όταν το χωρίο δεν είναι τόσο απλό όσο ένα ορθογώνιο το πρόβλημα εν γένει δεν είναι δυνατό να λυθεί ακριβώς αυτό το πρόβλημα που φέρει το όνομα 'πρόβλημα χωρισμού σε διμερή' (dimer problem). Δείτε για παράδειγμα το άρθρο [27].

4 Θεωρητική Επιστήμη Υπολογιστών

4.1 Πιθανοθεωρητικοί (randomized) αλγόριθμοι

Η χρήση μιας πηγής τυχαίων αριθμών σε ένα αλγόριθμο έχει αποδειχθεί πολλές φορές πως μπορεί να βοηθήσει στο να φτιαχτεί ένας αλγόριθμος αποτελεσματικός και απλός στην ανάλυσή του [23, 7]. Πολλές φορές ο καλύτερος γνωστός πιθανοθεωρητικός αλγόριθμος για ένα πρόβλημα είναι και καλύτερος και απλούστερος από τον καλύτερο *γνωστό* ντετερμινιστικό αλγόριθμο για το ίδιο πρόβλημα.

Η χρήση των πιθανοθεωρητικών αλγορίθμων δημιουργεί επίσης διάφορα αρκετά σημαντικά ερωτηματικά, όπως π.χ. το αν όντως το να επιτρέψει κανείς τη χρήση πιθανοθεωρητικών αλγορίθμων επιτρέπει την ύπαρξη αλγορίθμων αποδεδειγμένα καλύτερων από *οποιουσδήποτε* ντετερμινιστικούς.

Συμβαίνει επίσης συχνά να ξεκινά κανείς από ένα πιθανοθεωρητικό αλγόριθμο και να τον μετατρέπει σε ντετερμινιστικό (derandomization) χωρίς μεγάλης απώλεια ταχύτητας. Οι μέθοδοι που χρησιμοποιούνται για αυτή

τη μετατροπή είναι διάφορες (μέθοδος των υπό συνθήκη πιθανοτήτων, μικροί χώροι πιθανότητας, περιορισμένη ανεξαρτησία, κ.ά.).

4.2 Αλγοριθμικός έλεγχος για το αν ένας αριθμός είναι πρώτος

Ένα από τα πλέον συναρπαστικά αποτελέσματα στη θεωρητική επιστήμη υπολογιστών τα τελευταία χρόνια είναι ένας αλγόριθμος (Αύγουστος 2002) που ανακαλύφθηκε και που αποφασίζει αν ένας φυσικός αριθμός x είναι πρώτος σε χρόνο που φράσσεται από ένα πολυώνυμο του n, όπου n είναι το πλήθος των (δεκαδικών, δυαδικών) ψηφίων του αριθμού x [1, 5].

Μέχρι το 2002 οι καλύτεροι γνωστοί αλγόριθμοι για να αποφασίζουμε αν ένας αριθμός είναι πρώτος κόστιζαν χρόνο ο οποίος ήταν σχεδόν εκθετικός ως προς το n. Μόνο πιθανοθεωρητικοί αλγόριθμοι, όπως ο αλγόριθμος Miller-Rabin έτρεχαν σε πολυσνυμικό χρόνο. Σημειωτέον ότι ο αλγόριθμος Miller-Rabin ήταν γνωστό ότι μπορούσε να μετατραπεί σε ντετερμινιστικό πολυωνυμικό αλγόριθμο, υπό την προϋπόθεση ότι ισχύει η γενικευμένη εικασία του Riemann (GRH), που όμως εξακολουθεί να παραμένει αναπόδεικτη.

Επίσης να τονίσουμε ότι το σχετικό πρόβλημα της *παραγοντοποίησης* ενός ακεραίου σε χρόνο πολυωνυμικό ως προς το πλήθος των ψηφίων του, εξακολουθεί να παραμένει ανοιχτό. Δεν υπάρχουν δηλ. ακόμη αλγόριθμοι που να παραγοντοποιούν ένα ακέραιο σε χρόνο πολυωνυμικό ως προς το πλήθος των ψηφίων του. (Και ίσως να είναι και καλύτερα έτσι μια και αν ποτέ αποδειχτεί ότι υπάρχουν τέτοιοι αλγόριθμοι, θα καταρρεύσουν σχεδόν όλες οι κρυπτογραφικές μέθοδοι.)

4.3 Πολυπλοκότητα κυκλωμάτων για boolean συναρτήσεις

Το κεντρικότερο ίσως πρόβλημα της θεωρητικής επιστήμης υπολογιστών σήμερα είναι η απόδειξη κάτω φραγμάτων για το χρόνο που χρειάζεται για να λυθεί αλγοριθμικά ένα πρόβλημα. Για τα περισσότερα προβλήματα για τα οποία γνωρίζουμε, π.χ., μόνο εκθετικούς αλγόριθμους για τη λύση τους, τα γνωστά κάτω φράγματα είναι συνήθως τελείως τετριμμένα (π.χ. γραμμικά). Αυτό είναι ένα τεράστιο κενό στη γνώση μας και οφείλεται στο ότι είναι πολύ ευκολότερο να *εφεύρει* κανείς ένα αλγόριθμο από το να αποδείξει ότι δεν υπάρχει τέτοιος με δεδομένη αποτελεσματικότητα χρόνου ή χώρου. Και αυτό γιατί ένας υπολογιστής (μηχανή Turing) είναι ένα πολύ περίπλοκο αντικείμενο μια και εξελίσσεται στο χρόνο.

Γι΄ αυτό προσπαθούμε να αποδείξουμε σημαντικά κάτω φράγματα απλουστεύοντας το υπολογιστικό μοντέλο. Ένα τέτοιο απλουστευμένο μοντέλο, ιδιαίτερο προσφιλές λόγω της απλότητάς του, είναι τα λογικά κυκλώματα (boolean circuits). Αυτά είναι δικτυώματα από λογικές πύλες (AND, OR, NOT) που παίρνουν είσοδο από κάποιες λογικές μεταβλητές $x_1, \ldots, x_n$, και πρέπει να υπολογίζουν μια λογική συνάρτηση αυτών, για παράδειγμα μπορούμε να ζητήσουμε το κύκλωμα να υπολογίζει τη συνάρτηση

$$\text{PARITY}(x_1, \ldots, x_n) = x_1 + \cdots + x_n,$$

όπου η πρόσθεση είναι πρόσθεση modulo 2, είναι δηλ. η άνω συνάρτηση ίση με 1 (true) αν και μόνο αν περιττός αριθμός από τις μεταβλητές εισόδου είναι true.

Ένα πολύ σημαντικό αποτέλεσμα της τελευταίας εικοσαετίας είναι αυτό των Furst, Saxe και Sipser [10] και Hastad [15], που λέει ότι η συνάρτηση PARITY που ορίσαμε παραπάνω είναι αδύνατο να υπολογιστεί από κυκλώματα οποιουδήποτε σταθερού βάθους (βάθος είναι η απόσταση στο δίκτυο του κυκλώματος ανάμεσα στην πύλη εξόδου και στις πύλες εισόδου) και πολυωνυμικού μεγέθους ως προς το n (μέγεθος ενός κυκλώματος είναι το πλήθος των πυλών που χρησιμοποιεί). Η μέθοδος είναι πιθανοθεωρητική και συνδυαστική αλλά το πρόβλημα έχει επίσης προσεγγιστεί και αλγεβρικά [4].

4.4 Κβαντικοί υπολογισμοί

Τα τελευταία είκοσι χρόνια έχει αρχίσει να μελετάται το κβαντικό μοντέλο υπολογισιμότητας [26]. Στο κλασικό μοντέλο, η κατάσταση του υπολογιστικού συστήματος (π.χ., τα περιεχόμενα της μνήμης και της κεντρικής

μονάδας επεξεργασίας σε ένα συνηθισμένο υπολογιστή) είναι ανά πάσα στιγμή δυνατό να περιγραφούν από μια πεπερασμένη λέξη. Η δε επόμενη κατάσταση έπεται μονοσήμαντα από την προηγούμενη.

Στο κβαντικό μοντέλο, σύμφωνα με τις απαιτήσεις της κβαντικής μηχανικής, η κατάσταση ενός συστήματος περιγράφεται όχι από κάτι πεπερασμένο αλλά από ένα διάνυσμα σε ένα *μιγαδικό* χώρο Hilbert, πεπερασμένης ή άπειρης διάστασης. Ακόμη δηλ. κι αν η διάσταση του χώρου είναι πεπερασμένη, μια κατάσταση δε μπορεί να περιγραφεί με πεπερασμένο αριθμό ψηφίων. Η δε μετάβαση από μια κατάσταση στην επόμενη γίνεται με πολλαπλασιασμό με ένα unitary τελεστή στο χώρο (και είναι συνεπώς *αντιστρέψιμη*, πράγμα που δεν ισχύει στον κλασικό υπλογισμό). Στο 'τέλος' του υπολογισμού πρέπει να γίνει μια *μέτρηση* (που στο κβαντικό μοντέλο είναι υπολογισμός μιας τετραγωνικής μορφής πάνω στην τρέχουσα κατάσταση–διάνυσμα) ώστε να μετατραπεί η πληροφορία σε κλασική μορφή.

Στο κβαντικό μοντέλο υπολογισμού μπορούν να υπάρξουν αλγόριθμοι που σίγουρα δεν υφίστανται κλασικά. Για παράδειγμα, ο αλγόριθμος του Grover [13] μπορεί να ψάξει μια *μη ταξινομημένη* λίστα με n στοιχεία σε χρόνο $O(\sqrt{n})$, πράγμα προφανέστατα αδύνατο με οποιοδήποτε κλασικό αλγόριθμο.

Επίσης ο Shor [29] έχει δείξει πώς μπορεί κανείς με ένα κβαντικό αλγόριθμο να παραγνροποιήσει ένα ακέραιο σε χρόνο πολυωνυμνικό στο πλήθος των ψηφίων του ακεραίου. Δεν είναι μέχρι σήμερα γνωστό αν υπάρχει τέτοιος κλασικός αλγόριθμος.

Φιλοσοφικά μιλώντας, τα παραπάνω είναι δυνατά με κβαντικούς υπολογιστές μια και αυτή έχουν τη δυνατότητα, από τη φύση τους, επεξεργάζονται ταυτόχρονα πολλά δυνατά μονοπάτια υπολογισμού, να είναι, όπως λέμε, ανά πάσα στιγμή σε ένα συνδυασμό καταστάσεων αντί σε μία μόνο.

Η μελέτη των κβαντικών αλγορίθμων παρουσιάζει μεγάλο μαθηματικό ενδιαφέρον, ιδιαίτερα από την πλευρά της ανάλυσης.

Αναφορές

[1] M. Agrawal, N. Kayal and N. Saxena, PRIMES is in P, IIT Kanpur, Preprint of August 8, 2002.

[2] N. Alon and J. Spencer, *The probabilistic method*,

[3] J. Beck and W. Chen, *Irregularities of distribution*, Cambridge Tracts in Mathematics, 89. Cambridge University Press, Cambridge, 1987. xiv+294 pp.

[4] R. Beigel, The polynomial method in circuit complexity, Structure in Complexity Theory Conference, IEEE, 1993.

[5] F. Bornemann, PRIMES is in P: a breakthrough for everyman, Notices of the Amer. Math. Soc., May 2003.

[6] B. Chazelle, *The discrepancy method. Randomness and complexity*, Cambridge University Press, Cambridge, 2000. xviii+463 pp.

[7] T. Cormen, C. Leiserson and R. Rivest, *Introduction to Algorithms*, The MIT Press, Cambridge, MA, 1993.

[8] P. Erdős, Problems and results in additive number theory, Colloque sur la Théorie des Nombres, (CBRM, Bruxelles), 127-137.

[9] P. Erdős, On sets of distances of n points, Amer. Math. Monthly **53** (1946), p. 248-250.

[10] M. Furst, J. Saxe and M. Sipser, Parity, circuits, and the polynomial-time hierarchy, Math. Systems Theory **17** (1984), p. 13-27.

[11] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton Univ. Press, 1981.

[12] T. Gowers, Additive and combinatorial number theory, Cambridge lecture notes.

[13] L. Grover, A fast quantum mechanical algorithm for database search, Proc. 28th Symposium on the Theory of Computation, ACM, 1996.

[14] H. Halberstam and K.F. Roth, *Sequences*, Springer, New York, 1983.

[15] J. Hastad, Almost optimal lower bounds for small depth circuits, Proc. 18th Symposium on the Theory of Computation, ACM, 1986, p. 6-12.

[16] J.-P. Kahane, Sur les polynômes a coefficients unimodulaires, Bull. London Math. Soc. **12** (1980), 321-342.

[17] P.W. Kasteleyn, The statistics of dimers on a lattice, I. The number of dimer arrangements on a quadratic lattice, Physica **27** (1961), p. 1209-1225.

[18] R. Kenyon, Introduction to the dimer model, Lecture notes.

[19] S. Konyagin, O probleme Littlewood'a, Izv. A.N. SSSR, ser. mat. 45, **2** (1981), 243-265.

[20] J.E. Littlewood, On polynomials $\sum^n \pm z^m, \sum^n e^{\alpha_m i}, z = e^{\theta i}$, J. London Math. Soc. **41** (1966), 367-376.

[21] J. Matoušek, *Geometric discrepancy. An illustrated guide*, Algorithms and Combinatorics, 18. Springer-Verlag, Berlin, 1999. xii+288 pp.

[22] O.C. McGehee, L. Pigno and B. Smith, Hardy's inequality and the L^1 norms of exponentials sums, Ann. Math. **113** (1981), 613-618.

[23] R. Motwani and P. Raghavan, *Randomized Algorithms*, Cambridge University Press, 1995.

[24] D.J. Newman, *Analytic number theory*, Springer.

[25] J. Pach and P.K. Agarwal, *Combinatorial geometry*, Wiley, New York, 1995.

[26] J. Preskill, Lecture notes on quantum computation, Caltech, 2000.

[27] J. Propp, Enumeration of matchings: problems and progress, preprint.

[28] U. Schöning and R. Pruim, *Gems of theoretical computer science*, Springer 1998.

[29] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comp. **26** (1997), p. 1484-1509.

[30] J. Spencer, Six standard deviations suffice,

[31] L. Székely, Crossing numbers and hard Erdős problems in discrete geometry, Combin. Prob. and Computing **6** (1997), p. 353-358.

[32] E. Szemeredi, On sets of integers containing no k elements in arithmetic progression, Acta Arith. . **27** (1975), p. 299-345.

[33] H. Temperley and M. Fisher, The dimer problem in statistical mechanics – an exact result, Phil. Mag. **6** (1961), p. 1061-1063.