Θεωρία Πλέγματος και Κρυπτογραφικές Εφαρμογές

Διπλωματική Εργασία από τον φοιτητή

Δεμπέλη Δημήτριο
ΑΜ: 99027

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

ΕΜΠ

Εξεταστική επιτροπή

Χ.Κουκουβίνος, καθηγητής ΕΜΠ

Α.Παπαιωάννου, αν. καθηγητής ΕΜΠ (επιβλέπων)

Π.Στεφανέας, λέκτορας ΕΜΠ

Περιεχόμενα

Summary

The object of this diploma thesis is to illustrate how lattices can be applied to modern cryptography. In order to do so , we discuss certain fundamental results from lattice theory as well as the famous lattice reduction algorithm LLL. Having developed the theoretical tools, we proceed to apply them in three cryptosystems (Merkle-Hellman, GGH,NTRU), showing how they are based on lattices and how the LLL algorithm can be used for their cryptanalysis.

Κεφάλαιο 1:Εισαγωγή

Η κρυπτογραφία ασχολείται με την επικοινωνία παρουσία αντιπάλων (adversaries). Δηλαδή με την ασφάλεια των επικοινωνιών, ώστε ακόμα και αν οι αντίπαλοι υποκλέψουν κάποιο μήνυμα να μην μπορέσουν να το διαβάσουν. Έως σχετικά πρόσφατα τα συμμετρικά ή διπλής κατεύθυνσης κρυπτοσυστήματα ήταν τα μόνα που χρησιμοποιούνταν. Στα κρυπτοσυστήματα αυτά η ασφάλεια βασίζεται στην μυστικότητα του κλειδιού. Εάν ο αντίπαλος με κάποιο τρόπο ανακαλύψει το κλειδί μπορεί να έχει πρόσβαση σε όλες τις επικοινωνίες μεταξύ των δύο οντοτήτων (principals).Μέχρι να γίνει καινούρια ανταλλαγή κλειδιών μεταξύ των δύο οντοτήτων καμιά επικοινωνία δεν είναι ασφαλής. Εδώ πρέπει να τονίσουμε ότι η ανταλλαγή κλειδιών συνήθως είναι δύσκολο να γίνει σε ασφαλές περιβάλλον επικοινωνίας και αυτό είναι ένα επιπλέον μειονέκτημα των συμμετρικών κρυπτοσυστημάτων.

Λύση στο πρόβλημα αυτό έδωσε η κρυπτογραφία δημοσίου κλειδιού (public key cryptography) που παρουσιάστηκε για πρώτη φορά το 1976 στην πρωτοποριακή εργασία των Diffie και Hellman με τίτλο "New Directions in Cryptography" .Σύμφωνα με αυτή μια οντότητα έχει δύο κλειδιά: ένα ιδιωτικό που γνωρίζει μόνο αυτή και ένα δημόσιο που έχουν πρόσβαση όλοι. Αν κάποια άλλη οντότητα θέλει να επικοινωνήσει μαζί της, τότε χρησιμοποιεί το δημόσιο κλειδί της πρώτης για την κρυπτογράφηση. Η αρχική οντότητα κάνει την αποκρυπτογράφηση χρησιμοποιώντας το ιδιωτικό της κλειδί. Αυτό επιτρέπει στις δύο οντότητες να συμφωνήσουν σε ένα τρίτο μυστικό κλειδί για ένα συμμετρικό κρυπτοσύστημα.(key exchange protocol).Στις μέρες μας αυτή είναι μια πολύ σημαντική εφαρμογή της κρυπτογραφίας δημοσίου κλειδιού(που στην πράξη είναι πολύ πιο αργή από την συμμετρική και άρα μη συμφέρουσα για μεγάλες ποσότητες δεδομένων).

Κεντρικό ρόλο στην κρυπτογραφία δημοσίου κλειδιού έχουν οι συναρτήσεις καταπακτής (trapdoor functions) ή συναρτήσεις μονής κατεύθυνσης με μυστική πόρτα.

Ορισμός 1.1) Μία συνάρτηση καταπακτής είναι μια οικογένεια αντιστρέψιμων συναρτήσεων f_k με τα παρακάτω χαρακτηριστικά:

1. δοθέντων k, x ο υπολογισμός της $y = f_k(x)$ είναι υπολογιστικά εύκολος
2. δοθέντων k, y ο υπολογισμός της $x = f_k^{-1}(y)$ είναι υπολογιστικά εύκολος
3. δοθέντος y ο υπολογισμός της $f_k(x)$ είναι υπολογιστικά αδύνατος

Η ποσότητα k ονομάζεται μυστική πόρτα ή καταπακτή και είναι η ποσότητα εκείνη που απαιτείται για να είναι δυνατή η αντιστροφή της f_k.

Σε ένα κρυπτοσύστημα που βασίζεται σε μία συνάρτηση καταπακτής η κρυπτογράφηση είναι υπολογιστικά εύκολη αλλά η αποκρυπτογράφηση από κάποιον που δεν έχει το ιδιωτικό κλειδί είναι υπολογιστικά αδύνατη.

Οι συναρτήσεις καταπακτής βασίζονται σε δύσκολα υπολογιστικά προβλήματα. Στην πράξη τα περισσότερα από αυτά τα προβλήματα βασίζονται στην θεωρία αριθμών. Δύο από τα πιο γνωστά και χρησιμοποιούμενα είναι η παραγοντοποίηση, όπου μας δίνεται ένας ακέραιος n και ζητάμε τους πρώτους παράγοντές του, και το πρόβλημα του διακριτού λογαρίθμου όπου ζητάμε έναν x τέτοιο ώστε $a^x = b \pmod n$ (τα a,b,n είναι γνωστά και $x \le n-2$).

Το γεγονός ότι τα περισσότερα προβλήματα είναι από την θεωρία αριθμών δεν είναι επιθυμητό. Μια σημαντική ανακάλυψη στη θεωρία αυτή θα ήταν καταστροφική για τα κρυπτοσυστήματα που βασίζονται σε αυτά. Εξάλλου ήδη από το 1994 ο Peter Shor παρουσίασε έναν αλγόριθμο που επιλύει το πρόβλημα της παραγοντοποίησης σε πολυωνυμικό χρόνο με χρήση κβαντικού υπολογιστή. Για αυτούς τους λόγους οι κρυπτογράφοι άρχισαν να αναζητούν και σε άλλες περιοχές των μαθηματικών δύσκολα προβλήματα προκειμένου να βασίσουν εκεί τις συναρτήσεις καταπακτής τους (post quantum cryptography) .

Μια από τις περιοχές των μαθηματικών που εξέτασαν οι κρυπτογράφοι είναι η θεωρία πλέγματος (lattice theory). Τα πλέγματα είναι διακριτές προσθετικές υποομάδες του R^n και η θεωρία τους είχε ήδη σημαντικές εφαρμογές στην κρυπτογραφία. Πράγματι ο αλγόριθμος αναγωγή πλέγματος (lattice reduction) LLL από τους Lenstra, Lenstra και Lovász είχε χρησιμοποιηθεί με επιτυχία για το σπάσιμο του κρυπτοσυστήματος Merkle-Hellman που βασίζεται στο πρόβλημα του σακιδίου (Knapsack problem). Το 1996 όμως, ο Ajtai με την εργασία του "Generating hard instances of lattice problems" έδειξε ότι η θεωρία πλέγματος μπορούσε να δώσει και συναρτήσεις καταπακτής για νέα κρυπτοσυστήματα.

Με την εργασία του αυτή ο Ajtai ικανοποίησε και έναν ακόμα στόχο των κρυπτογράφων: να βρεθεί ένα δύσκολο πρόβλημα που να γνωρίζουμε την σχέση μεταξύ της δυσκολίας τυχαίων στιγμιοτύπων και τις δυσκολίας των στιγμιοτύπων της χειρότερης περίπτωσης. Για κανένα άλλο κρυπτογραφικό πρόβλημα δεν είναι γνωστή αυτή η σχέση. Πιο συγκεκριμένα η εργασία του παρουσιάζει ένα συγκεκριμένο τυχαίο πρόβλημα, που αφορά μια κλάση τυχαίων πλεγμάτων, η λύση του οποίου οδηγεί στη λύση των ακόλουθων βασικών προβλημάτων της θεωρίας πλέγματος:

1. Εύρεση του μήκους του μικρότερου μη μηδενικού διανύσματος σε ένα πλέγμα διάστασης n προσεγγιστικά, ως ένα πολυωνυμικό παράγοντα.
2. Εύρεση του μικρότερου μη μηδενικού διανύσματος σε ένα πλέγμα διάστασης n. Επιπλέον απαιτούμε το διάνυσμα αυτό, έστω u, να είναι μοναδικό δηλαδή κάθε άλλο διάνυσμα με μήκος το πολύ $n^c \|u\|$ να είναι παράλληλο στο u, με c μια αρκετά μεγάλη θετική σταθερά.
3. Εύρεση μιας βάσης $b_1, \ldots, b_n$ ενός πλέγματος διάστασης n της οποίας το μήκος, που είναι ίσο με $\max_{i=1,\ldots,n} \|b_i\|$ είναι το μικρότερο δυνατό.

Δυστυχώς το κρυπτοσύστημα του Ajtai δεν είναι λειτουργικό στην πράξη. Η θεωρητική του επιτυχία όμως ήταν το έναυσμα για την δημιουργία πιο πρακτικών κρυπτοσυστημάτων όπως το GGH και το NTRU τα οποία θα μελετήσουμε στην εργασία αυτή.

Εξάλου, το 1996 ο Coppersmith χρησιμοποίησε με επιτυχία την αναγωγή πλέγματος για την εύρεση μικρών ριζών πολυωνυμικών εξισώσεων μικρού βαθμού. Τα αποτελέσματά του χρησιμοποιήθηκαν σε επιθέσεις εναντίον του RSA και στην παραγοντοποίηση ακεραίων ειδικής μορφής.

Συμπερασματικά, η θεωρία πλέγματος είναι από τις πιο «ζωντανές» περιοχές των μαθηματικών που χρησιμοποιούνται στην κρυπτογραφία. Σκοπός της εργασίας αυτής είναι να αναδείξει τα βασικά στοιχεία της μαθηματικής θεωρίας, να παρουσιάσει αλγόριθμους επίλυσης των βασικών προβλημάτων της και να περιγράψει ορισμένες κρυπτογραφικές εφαρμογές της. Το υπόλοιπο της εργασίας διαρθρώνεται ως εξής:

1. Το δεύτερο κεφάλαιο κάνει μια επιγραμματική αναφορά σε βασικά στοιχεία της θεωρίας πολυπλοκότητας που θα χρειαστούν στη συνέχεια. Ακόμα

παρουσιάζει τα δύσκολα προβλήματα της θεωρίας πλέγματος που χρησιμοποιούνται στην κρυπτογραφία και την πολυπλοκότητα τους.

2. Το τρίτο κεφάλαιο παρουσιάζει τα κύρια στοιχεία των μαθηματικών της θεωρίας πλέγματος και ορισμένα στοιχεία από την άλγεβρα που χρειάζονται για το NTRU.
3. Το τέταρτο κεφάλαιο παρουσιάζει την αναγωγή πλέγματος (lattice reduction) με βάση τον αλγόριθμο LLL και κάνει αναφορά στην αναγωγή κατά block (BKZ-LLL).
4. Το πέμπτο κεφάλαιο παρουσιάζει ορισμένες από τις κρυπτογραφικές εφαρμογές της θεωρίας. Εστιάζουμε στα Knapsacks,στο GGH και κυρίως στο NTRU που είναι το πιο σύγχρονο και το πιο χρησιμοποιούμενο.

Κεφάλαιο 2) Δύσκολα προβλήματα στη θεωρία πλέγματος

2.1) Στοιχεία από την Θεωρία Πολυπλοκότητας.

Ξεκινάμε το κεφάλαιο αυτό με ορισμένες βασικές έννοιες από την Θεωρία Πολυπλοκότητας.

Ορισμός 2.1) Πολυωνυμικός Χρόνος
Ένας αλγόριθμος τρέχει σε πολυωνυμικό χρόνο αν ο αριθμός βημάτων μιας μηχανής Turing ή ο αριθμός των πράξεων bit φράσσεται πολυωνυμικά στο μήκος της εισόδου. Δηλαδή

Αριθμός Βημάτων Εισόδου = poly (μήκος εισόδου)

Ένας αλγόριθμος που τρέχει σε πολυωνυμικό χρόνο ονομάζεται αποδοτικός.

Υπενθυμίζουμε ότι μια δυαδική ακολουθία γίνεται αποδεκτή από έναν αλγοριθμο A αν A(x)=1, δηλαδή για είσοδο x ο αλγόριθμος βγάζει στην έξοδο 1. Αν A(x)=0 λέμε ότι ο αλγόριθμος απορρίπτει τη δυαδική ακολουθία. Μια γλώσσα L είναι ένα σύνολο δυαδικών ακολουθιών (ή πιο γενικά μια γλώσσα L είναι ένα σύνολο ακολουθιών πάνω σε κάποιο αλφάβητο Σ). Η γλώσσα L που γίνεται δεκτή από έναν αλγόριθμο A είναι : $L = \{x \in \{0,1\}^* : A(x) = 1\}$. Λέμε ότι μια γλώσσα L αποκρίνεται από έναν αλγόριθμο A αν κάθε δυαδική ακολουθία της L γίνεται αποδεκτή από τον A και κάθε δυαδική ακολουθία που δεν ανήκει στην L απορρίπτεται από τον A. Η έννοια της απόκρισης είναι ισχυρότερη από την έννοια της αποδοχής. Πράγματι, ακόμα και αν μια γλώσσα L γίνεται αποδεκτή από έναν αλγόριθμο A, δεν μπορούμε να είμαστε βέβαιοι ότι μια δυαδική ακολουθία x, που δεν ανήκει στην L θα απορριφθεί από αυτόν. Μπορεί για παράδειγμα, ο αλγόριθμος να εισέλθει σε έναν ατέρμονα βρόγχο (endless loop).

Με βάση τα παραπάνω μπορούμε να ορίσουμε την κλάση πολυπλοκότητας P

Ορισμός 2.2) Κλάση πολυπλοκότητας P

Η κλάση P ορίζεται $P = \left\{ \begin{array}{l} L \subseteq \{0,1\}^* : \text{υπάρχει αλγόριθμος A που αποκρίνεται} \\ \text{για την L σε πολυωνυμικό χρόνο} \end{array} \right\}$

Ένας αλγόριθμος επαλήθευσης (verification algorithm) είναι ένας αλγόριθμος που δέχεται δύο παράγοντες (ορίσματα) ως είσοδο: το πρώτο όρισμα είναι μια συνηθισμένη δυαδική ακολουθία x , ενώ το δεύτερο μια δυαδική ακολουθία y που λέγεται πιστοποιητικό. Λέμε ότι ένας αλγόριθμος επαλήθευσης A επαληθεύει μια δυαδική ακολουθία x αν υπάρχει ένα πιστοποιητικό y τέτοιο ώστε A(x,y) = 1. Η γλώσσα που επαληθεύεται από έναν αλγόριθμο επαλήθευσης A είναι η :

$$L = \{x \in \{0,1\}^* : \text{υπάρχει } y \in \{0,1\}^* \text{ τέτοιο ώστε } A(x, y) = 1\}$$

Με βάση τα παραπάνω ορίζουμε την κλάση πολυπλοκότητας NP

Ορισμός 2.3) Κλάση πολυπλοκότητας NP

Λέμε ότι μια γλώσσα ανήκει στην κλάση πολυπλοκότητας NP αν και μόνο αν υπάρχει ένας αλγόριθμος επαλήθευσης Α και μια σταθερά c τέτοια ώστε : $L = \left\{ x \in \{0,1\}^* : \text{υπάρχει ένα πιστοποιητικό y με } |y| = O\left(|x|^c\right) \text{τέτοιο ώστε A(x, y)} = 1 \right\}$
Τότε λέμε ότι ο αλγόριθμος Α επαληθεύει την γλώσσα L σε πολυωνυμικό χρόνο.

Είναι εύκολο να δούμε ότι $P \subseteq NP$. Πράγματι για μια γλώσσα $L \in P$ έχουμε έναν αλγόριθμο Α που αποκρίνεται για τη γλώσσα. Τροποποιώντας τον αλγόριθμο ώστε να δέχεται και ένα δεύτερο όρισμα σαν πιστοποιητικό (ο αλγόριθμος θα αγνοεί το δεύτερο όρισμα αφού μπορεί από το πρώτο και μόνο όρισμα να αποφασίσει ποιες δυαδικές ακολουθίες ανήκουν στην γλώσσα L) , παίρνουμε έναν αλγόριθμο επαλήθευσης για την γλώσσα L. Άρα $L \in NP$ και $P \subseteq NP$. Το αν $NP \subseteq P$ και κατά συνέπεια $P = NP$ είναι ανοικτό πρόβλημα και βρίσκεται στην καρδιά της θεωρίας πολυπλοκότητας. Πιστεύεται ότι $P \neq NP$. Αυτό μπορούμε να το καταλάβουμε διαισθητικά ως εξής:

Ορισμός 2.4) Αναγωγή κατά Karp
Λέμε ότι ένα πρόβλημα Α ανάγεται πολυωνυμικά κατά Karp σε ένα πρόβλημα Β και συμβολίζουμε $A \leq_m^p B$, τότε και μόνον τότε, όταν υπάρχει μια συνάρτηση f υπολογίσιμη σε πολυωνυμικό χρόνο ώστε $x \in A \Leftrightarrow f(x) \in B$, $\forall x \in A$.

Μια πιο γενική μορφή αναγωγής είναι η αναγωγή κατά Cook.

Ορισμός 2.5) Αναγωγή κατά Cook
Λέμε ότι ένα πρόβλημα Α ανάγεται κατά Cook σε ένα πρόβλημα Β και συμβολίζουμε $A \leq_T^P B$, αν το Α μπορεί να αποφασιστεί από μια πολυωνυμικού χρόνου ντετερμινιστική μηχανή Turing η οποία χρησιμοποιεί ένα μαντείο (oracle) για το Β. Αυτό σημαίνει ότι η DTM μπορεί να κάνει όσες ερωτήσεις θέλει για οποιαδήποτε στιγμιότυπο του Β και να πάρει σωστές απαντήσεις με κόστος O(1).

Ορισμός 2.6) NP-πλήρη προβλήματα
Μια γλώσσα $L \subseteq \{0,1\}^*$ είναι NP-πλήρης αν ικανοποιούνται οι εξής δύο ιδιότητες:

1. $L \in NP$
2. $L' \leq_m^p L$, $\forall L' \in NP$

Αν μια γλώσσα ικανοποιεί την ιδιότητα (2) αλλά όχι απαραίτητα την ιδιότητα (1) τότε λέμε ότι η γλώσσα αυτή είναι NP-δύσκολη (NP-hard) και το αντίστοιχο πρόβλημα NP-δύσκολο.

Τα NP-πλήρη προβλήματα είναι τα πιο δύσκολα στην κλάση NP με την έννοια ότι αν κάποιο από αυτά βρεθεί να είναι στην κλάση P τότε $P = NP$. Πράγματι έστω $L \in P$ και L NP-πλήρη. Τότε $\forall L' \in NP$ έχουμε $L' \leq_m^p L$ από την ιδιότητα (2) άρα $L' \in P$ άρα $NP \subseteq P$ δηλαδή $P = NP$.

Παραθέτουμε μερικά NP-πλήρη προβλήματα:

- **Το πρόβλημα SAT :** Δίνεται μια boolean έκφραση σε CNF (Conjuctive Normal Form) και ζητείται αν υπάρχει ανάθεση τιμών στις μεταβλητές

που να ικανοποιεί την έκφραση (δηλαδή η έκφραση να αποτιμάται ως αληθής (TRUE)).

- **Το πρόβλημα 3-SAT :** Δίνεται μια boolean έκφραση σε 3-CNF (δηλαδή σε CNF της οποίας κάθε clause έχει ακριβώς 3 (διαφορετικά) literals). Ζητείται αν υπάρχει ανάθεση τιμών στις μεταβλητές που να ικανοποιεί την έκφραση.
- **Το πρόβλημα του αθροίσματος υποσυνόλου (SUBSET SUM) :** Δίνονται τα $n, a_1, a_2, ..., a_n, b \in \mathrm{N}$ και ζητείται $x \in \{0,1\}^n$ τέτοιο ώστε $\sum_{i=1}^{n} a_i x_i = b$

Φυσικά υπάρχουν και πολλά άλλα NP-πλήρη προβλήματα. Για κανένα από όλα αυτά δεν έχει βρεθεί αποδοτικός αλγόριθμος. Έτσι τα προβλήματα αυτά είναι η πιο σημαντική πρακτική ένδειξη ότι $P \neq NP$.

Επειδή πολλά από τα NP-πλήρη προβλήματα έχουν σημαντικές εφαρμογές, και δεν υπάρχει αποδοτικός αλγόριθμος για την λύση τους, στην πράξη λύνονται με προσεγγιστικούς αλγορίθμους πολυωνυμικού χρόνου. Οι προσεγγιστικοί αλγόριθμοι εφαρμόζονται σε προβλήματα βελτιστοποίησης. Αυτό σημαίνει ότι για να τους χρησιμοποιήσουμε μετατρέπουμε τα προβλήματα απόφασης (όπου ζητάμε ένα ΝΑΙ ή ΟΧΙ) σε προβλήματα βελτιστοποίησης (όπου ζητάμε το ελάχιστο ή το μέγιστο μιας ποσότητας). Κάθε πιθανή λύση σε ένα πρόβλημα βελτιστοποίησης έχει ένα (θετικό) κόστος. Όσο μεγαλύτερο είναι το κόστος μιας λύσης για ένα πρόβλημα μεγιστοποίησης ή όσο μικρότερο για ένα πρόβλημα ελαχιστοποίησης, τόσο η λύση αυτή προσεγγίζει τη βέλτιστη (που έχει μέγιστο ή ελάχιστο κόστος αντίστοιχα) .

Ορισμός 2.7) Προσεγγιστικός αλγόριθμος, λόγος προσέγγισης
Έστω ότι έχουμε έναν αλγόριθμο Α που για είσοδο μεγέθου n μας δίνει λύση για ένα πρόβλημα βελτιστοποίησης κόστους C ενώ ο βέλτιστος αλγόριθμος μας δίνει λύση κόστους C^*. Τότε λέμε ότι ο αλγόριθμος Α έχει λόγο προσέγγισης $p(n)$ αν $\max\left(\frac{C}{C^*}, \frac{C^*}{C}\right) \leq p(n)$. Ο Α λέγεται $p(n)$-προσεγγιστικός αλγόριθμος .

Ισχύει $p(n) \geq 1$. Αν $p(n) = 1$ ο αλγόριθμος είναι βέλτιστος. Σε ορισμένες περιπτώσεις μπορούμε να έχουμε καλύτερο λόγο προσέγγισης με αντάλλαγμα περισσότερο υπολογιστικό χρόνο ή το αντίστροφο. Τότε κάνουμε λόγο για σχήματα προσέγγισης (approximation schemes).

Ορισμός 2.8) Σχήμα προσέγγισης.
Ένα σχήμα προσέγγισης για ένα πρόβλημα βελτιστοποίησης είναι ένας προσεγγιστικός αλγόριθμος που ως είσοδο δέχεται ένα στιγμιότυπο του προβλήματος και μια θετική σταθερά ε $(\varepsilon > 0)$ και ως έξοδο βγάζει μια $(1+\varepsilon)$ προσέγγιση της βέλτιστης λύσης προκειμένου για πρόβλημα ελαχιστοποίησης ή μία $\frac{1}{1+\varepsilon}$ προσέγγιση προκειμένου για πρόβλημα μεγιστοποίησης. Αν για δεδομένο ε το σχήμα προσέγγισης έχει πολυωνυμικό

χρόνο τρεξίματος ως προς n (n το μέγεθος της εισόδου) τότε λέγεται σχήμα προσέγγισης πολυωνυμικού χρόνου (PTAS).

Ορισμός 2.9) Σχήμα προσέγγισης πλήρως πολυωνυμικού χρόνου (FPTAS)
Ένα σχήμα προσέγγισης πλήρως πολυωνυμικού χρόνου είναι ένα σχήμα προσέγγισης με χρόνο τρεξίματος πολυωνυμικό ως προς το n και το $\frac{1}{\varepsilon}$.

Για παράδειγμα ένα PTAS μπορεί να έχει χρόνο τρεξίματος $O\left(n^{\frac{1}{\varepsilon}}\right)$ ενώ ένα FPTAS $O\left(\frac{n}{\varepsilon}\right)$.

2.2) Δύσκολα προβλήματα στη θεωρία πλέγματος και η πολυπλοκότητά τους

Δίνουμε έναν ορισμό του πλέγματος

Ορισμός 2.10) Πλέγμα
Έστω $b_1, b_2, ..., b_n \in \Re^m$ γραμμικά ανεξάρτητα διανύσματα. Ονομάζουμε την προσθετική υποομάδα $L(b_1, b_2, ..., b_n) = \left\{ \sum_{i=1}^{n} b_i t_i \middle| t_1, ..., t_m \in Z \right\} = \sum_{i=1}^{n} b_i Z$ του $\Re^m$ πλέγμα με βάση τα $b_1, b_2, ..., b_n$. Ο βαθμός ή διάσταση του πλέγματος είναι rank(L)=n.

Δοθείσης μιας βάσης $b_1, b_2, ..., b_n \in Z^m$ για ένα πλέγμα L τα ακόλουθα θεωρούνται υπολογιστικά δύσκολα προβλήματα:

a) Εύρεση του μικρότερου μη τετριμμένου διανύσματος του πλέγματος
b) Εύρεση μιας βάσης που αποτελείται από μικρά διανύσματα
c) Για δεδομένο διάνυσμα $z \in \Re^n$ να βρεθεί το πλησιέστερο διάνυσμα που ανήκει στο πλέγμα

Το (a) λέγεται πρόβλημα του μικρότερου διανύσματος (Shortest Vector Problem) και θα το αναφέρουμε ως SVP. Ο μαθηματικός ορισμός του είναι:

Ορισμός 2.11) Shortest Vector Problem – SVP
Δοθείσης μιας βάσης ενός πλέγματος L ζητείται να βρεθεί ένα διάνυσμα $u \in L$ τέτοιο ώστε $\|u\| = \|L\|$. Στην προσεγγιστική μορφή του προβλήματος (apprSVP) ζητείται $\|u\| \le f(d) \cdot \|L\|$ όπου $f(d)$ ο παράγοντας προσέγγισης.

Το (b) λέγεται πρόβλημα της μικρότερης βάσης (Shortest Basis Problem) και θα το αναφέρουμε σαν SBP.

Ορισμός 2.12) Shortest Basis Problem-(SBP)
Δοθέντος ενός πλέγματος να βρεθεί μία βάση $\{b_1,b_2,\ldots,b_n\}$ που να είναι η μικρότερη με βάση κάποιο κριτήριο που έχουμε επιλέξει. Τέτοιο κριτήριο μπορεί για παράδειγμα να είναι τα b_i να είναι τέτοια ώστε το $\max_{1\le i\le n} \|b_i\|$ ή το $\sum^{n}_{i=1}\|b_i\|^2$ να είναι ελάχιστο. Επομένως ανάλογα με το κριτήριο που έχουμε επιλέξει έχουμε και μια διαφορετική εκδοχή του SBP.

Το (c) λέγεται πρόβλημα του πλησιέστερου διανύσματος (Closest Vector Problem) και θα το αναφέρουμε ως CVP. Πρόκειται για την μη ομογενή μορφή του SVP.

Ορισμός 2.13) Closest Vector Problem – CVP
Δοθείσης μιας βάσης ενός πλέγματος L και ενός διανύσματος $v \in \Re^n$ ζητείται να βρεθεί το πλησιέστερο διάνυσμα στο v που ανήκει στο πλέγμα. Δηλαδή ζητείται ένα διάνυσμα $u \in L$ τέτοιο ώστε $\forall w \in L \ \ \|u-v\| = \|w-v\|$. Στην προσεγγιστική μορφή του προβλήματος (apprCVP) ζητάμε $u \in L$ τέτοιο ώστε $\forall w \in L$ $\|u-v\| \le f(d)\cdot\|w-v\|$, όπου $f(d)$ ο λόγος προσέγγισης.

Στην εργασία αυτή θα ασχοληθούμε με το SVP και το CVP.Και τα δύο αυτά προβλήματα θεωρούνται γενικά υπολογιστικά δύσκολα. Όμως η νόρμα που χρησιμοποιείται για την απόσταση παίζει καθοριστικό ρόλο για το πόσο δύσκολο είναι το πρόβλημα. Για παράδειγμα το SVP είναι NP-complete για $\|\ \|_\infty$ ενώ για την ℓ_2 νόρμα ο Ajtai έχει δείξει ότι το SVP είναι NP-hard μέσω τυχαιοποιημένων αναγωγών. Το CVP θεωρείται πιο δύσκολο από το SVP και μάλιστα είναι NP-complete για κάθε νόρμα. Επιπλέον, τόσο το SVP όσο και το CVP είναι δύσκολο να προσεγγιστούν. Με αυτό εννοούμε ότι δεν υπάρχει πολυωνυμικός αλγόριθμος που να τα προσεγγίζει με λόγο προσέγγισης πολυωνυμικό ως προς τη διάσταση του πλέγματος. Ο αλγόριθμος LLL προσεγγίζει το SVP με λόγο $2^{(m-1)/2}$ όπου m η διάσταση του πλέγματος. Ο καλύτερος προσεγγιστικός αλγόριθμος για το SVP είναι τυχαιοποιημένος και έχει λόγο προσέγγισης $2^{O(m\log\log m/\log m)}$ (από τους Ajtai, Kumar και Sivakumar). Ο καλύτερος αλγόριθμος για ακριβή λύση, επίσης από τους Ajtai, Kumar και Sivakumar, θέλει χρόνο $2^{O(m)}$ (επίσης τυχαιοποιημένος). Για το CVP, ο καλύτερος για ακριβή λύση, από τον Kannan, θέλει χρόνο $2^{O(m\log m)}$. Ο Babai με τον αλγόριθμο LLL, προσέγγισε το CVP με λόγο $2^{m/2}$. Ο καλύτερος προσεγγιστικός αλγόριθμος από τους Ajtai, Kumar και Sivakumar έχει λόγο $2^{O(m\log\log m/\log m)}$.

Κεφάλαιο 3)Μαθηματική Θεωρία

3.1)Διανυσματικοί χώροι

Ξεκινάμε το κεφάλαιο υπενθυμίζοντας ορισμένα βασικά στοιχεία από τη θεωρία διανυσματικών χώρων και τη θεωρία πινάκων.

Διανυσματικός χώρος: Ένας διανυσματικός χώρος V είναι ένα υποσύνολο του R^m με την ιδιότητα το $a_1v_1+a_2v_2$ να ανήκει στο V για όλα τα v_1,v_2 που ανήκουν στο V και όλα τα a_1,a_2 που ανήκουν στο R. Δηλαδή το V είναι κλειστό ως προς την πρόσθεση και το βαθμωτό πολλαπλασιασμό από στοιχεία του R. Ένα διάνυσμα της μορφής $w=a_1v_1+a_2v_2+\ldots+a_nv_n$ με τα a_i να ανήκουν στο R λέγεται γραμμικός συνδυασμός των v_i.Το σύνολο όλων των γραμμικών συνδυασμών λέγεται γραμμική θήκη (των $\{v_1,v_2,\ldots,v_n\}$) και συμβολίζεται με

$$\text{span}(\{v_1,v_2,\ldots,v_n\})$$

Ένα πεπερασμένο σύνολο διανυσμάτων $B=\{v_1,v_2,\ldots,v_n\}$ λέγεται βάση του V αν span(B)=V (δηλαδή κάθε διάνυσμα x του V γράφεται με μοναδικό τρόπο σαν $x=a_1v_1+a_2v_2+\ldots+a_nv_n$ και τα διανύσματα του B είναι γραμμικά ανεξάρτητα, δηλαδή Bx=0 αν και μόνο αν x=0. Διάσταση του διανυσματικού χώρου λέγεται ο αριθμός των διανυσμάτων της βάσης του. Ισχύει η εξής πρόταση: Έστω $\{v_1,v_2,\ldots,v_n\}$μία βάση του V και $w_1,w_2,\ldots,w_n$ διανύσματα του V.Γράφουμε τα w_i σαν γραμμικούς συνδυασμούς των v_i δηλαδή $w_i=a_{i1}v_1+a_{i2}v_2+\ldots+a_{in}v_n$.Τότε τα $\{w_1,w_2,..,w_n\}$ είναι βάση του V αν και μόνο αν η ορίζουσα του πίνακα των συντελεστών w_i είναι διάφορη του μηδενός. Εδώ θα ενδιαφερθούμε για πεπερασμένους διανυσματικούς χώρους πάνω στο $\Re$ ή στο Q. Μας ενδιαφέρει επίσης η μέτρηση μήκους στον R^m και σε υποσύνολά του, όπως και η γωνία μεταξύ δύο διανυσμάτων . Αυτό μας οδηγεί στον ορισμό της νόρμας και του εσωτερικού γινομένου.

Μία νόρμα $\|.\|$ από το V στο $\Re$ ικανοποιεί τις ακόλουθες ιδιότητες:

1) $\|x\| \geq 0$ και $\|x\| = 0$ αν και μόνο αν x = 0.

2) $\|a \cdot x\| = |a| \cdot \|x\|$.

3) $\|x + y\| \leq \|x\| + \|y\|$.

Οι βασικές νόρμες είναι:

1)Η ℓ_1 νόρμα : $\|x\|_1 = \sum_{i=1}^{n} |x_i|$

2)Η ℓ_2 νόρμα: $\|x\|_2 = \sqrt{\langle x, x \rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}$

3)Η ℓ_∞ νόρμα: $\|x\|_\infty = \max_{i=1}^{n} |x_i|$

4)Η ℓ_p νόρμα: $\left(\sum_{i=1}^{n} |x_i|^p \right)^{1/p}$

Ορίζουμε ως εσωτερικό γινόμενο $\langle .,. \rangle$ την απεικόνιση $\langle .,. \rangle : V^n \text{ x } V^n \to \Re$ που ικανοποιεί τις ακόλουθες ιδιότητες για κάθε u , v , w $\in V^n$ και για κάθε $\lambda \in \Re$:

1) $\langle .,. \rangle$ είναι διγραμμική; $\langle u+w, v \rangle = \langle u, v \rangle + \langle v, w \rangle$

$\langle \lambda u, v \rangle = \lambda \langle u, v \rangle$

$\langle u, v+w \rangle = \langle u, v \rangle + \langle v, w \rangle$

$\langle u, \lambda v \rangle = \lambda \langle u, v \rangle$

2) $\langle .,. \rangle$ είναι συμμετρική: $\langle u, v \rangle = \langle v, w \rangle$

3) $\langle .,. \rangle$ είναι θετικά ορισμένη : $\langle u, u \rangle \rangle 0$ για $u \neq 0$

Το σύνηθες εσωτερικό γινόμενο ορίζεται ως :

$$\left\langle (u_1, u_2, ..., u_n)^T, (v_1, v_2, ..., v_n)^T \right\rangle = \sum_{i=1}^{n} u_i v_i$$

Λέμε ότι δύο διανύσματα x, y είναι ορθογώνια (ή κάθετα μεταξύ τους) και συμβολίζουμε με $(x \perp y)$ όταν $\langle x, y \rangle = 0$. Μία βάση $\{v_1, v_2, \ldots, v_n\}$ λέγεται ορθογώνια όταν $\langle v_i, v_j \rangle = 0$ για όλα τα $i \neq j$.

Μία νόρμα επάγει το (αντίστοιχο) εσωτερικό γινόμενο: $\|u\| = \sqrt{\langle u, u \rangle}$.Για κάθε νόρμα και το αντίστοιχο εσωτερικό της γινόμενο (με u , v $\in V^n$) ικανοποιούν την ανισότητα Cauchy-Schwarz : $|\langle u, v \rangle| \leq \|u\| \cdot \|v\|$ με την ισότητα να ισχύει όταν τα δύο διανύσματα είναι γραμμικά εξαρτημένα ή το ένα από τα δύο να είναι το μηδενικό διάνυσμα. Για $v \neq 0$ έχουμε $f(t)=\|u-tv\|^2=(u-tv)\cdot(u-tv)=u\cdot u-2tu\cdot v+t^2 v\cdot v=\|u\|^2-2tu\cdot v+t^2\|w\|^2$.Όμως $f(t)\geq 0$ για κάθε πραγματικό t και η τιμή που ελαχιστοποιεί την f είναι $t=(u\cdot v)/\|v\|^2$.Αντικαθιστώντας παίρνουμε $\|u\|^2-((u\cdot v)^2/\|v\|^2)\geq 0$ και τελικά την ζητούμενη ανισότητα.

Ο δυϊκός ενός διανυσματικού χώρου V πάνω σε ένα σώμα F είναι το σύνολο όλων των γραμμικών τελεστών από το V στο και συμβολίζεται με $\tilde{V}$.Ο δυϊκός $\tilde{V}$ είναι επίσης ένας διανυσματικός χώρος πάνω στο F και μάλιστα είναι ισομορφικός με τον V.

Ένας τετραγωνικός πίνακας $A \in \Re^{nxn}$ λέγεται ιδιάζων αν det(A)=0 ή ισοδύναμα οι γραμμές τους ή οι στήλες τους είναι γραμμικά ανεξάρτητες. Σύμφωνα με τον κανόνα του Crammer για κάθε μη ιδιάζοντα πίνακα $A=[a_1,\ldots,a_n] \in \Re^{nxn}$ και $b \in \Re^n$ τότε η μοναδική λύση του συστήματος Ax=b δίνεται από:

$$x_i = \frac{\det([a_1, ..., a_{i-1}, b, a_{i+1}, ..., a_n])}{\det(A)}$$

Παρατηρούμε ότι αν ο A και το b είναι ακέραιοι τότε και το det(A)x είναι ακέραιο διάνυσμα, όπου x είναι η μοναδική λύση του συστήματος.

Ορισμός 3.1)Ένας τετραγωνικός πίνακας U λέγεται unimodular αν det(U)=±1 και τα στοιχεία του είναι ακέραιοι. Από τον κανόνα του Crammer συμπεραίνουμε ότι ο αντίστροφος ενός unimodular πίνακα είναι και αυτός unimodular.Συμβολίζουμε το σύνολο όλων των unimodular πινάκων διάστασης n με $GL_n(Z)$ δηλαδή:

$$GL_n(Z) := \{ A \in M_{n,n}(Z) \mid \det(A) = \pm 1 \}$$

Έστω $S, T \in GL_n(Z)$ τότε αφού $\det(ST)=\det(S) \bullet \det(T)$ ο πίνακας $S \bullet T$ ανήκει στην $GL_n(Z)$.
Επίσης ο μοναδιαίος πίνακας είναι unimodular.
Τέλος, αν $T \in GL_n(Z)$ τότε έχουμε: $\det(T^{-1}) = \dfrac{1}{\det(T)}$
άρα: $\det(T^{-1}) = \pm 1$
και από τον κανόνα του Crammer το (i,j) στοιχείο στον T^{-1} είναι: $\dfrac{(-1)^{i+j} \bullet \det(T_{ij})}{\det(T)} = \pm \det(T_{ij})$, όπου T_{ij} είναι ο T που του έχουμε αφαιρέσει την i-οστη γραμμή και την j-οστη στήλη. Επειδή ο T_{ij} είναι ακέραιος πίνακας έχουμε ότι και ο $\det(T_{ij})$ είναι ακέραιος αριθμός. Επομένως για $T \in GL_n(Z)$ έχουμε ότι $T^{-1} \in GL_n(Z)$.
Από τα παραπάνω συμπεραίνουμε ότι η $GL_n(Z)$ είναι ομάδα.

Μία βασική ιδιότητα των unimodular πινάκων είναι ότι οι ακόλουθες πράξεις επί γραμμών πίνακα μπορούν να γίνουν σε έναν πίνακα απλά πολλαπλασιάζοντάς τον από δεξιά με έναν κατάλληλο unimodular πίνακα:

- Πολλαπλασιασμός μιας στήλης με -1
- Εναλλαγή δύο στηλών
- Πολλαπλασιασμός μιας στήλης με έναν ακέραιο αριθμό και πρόσθεση σε άλλη στήλη

3.2)Ορθοκανονικοποίηση Gram-Schmidt και ανισότητα Hadamard

Η ορθοκανονικοποίηση Gram-Schmidt είναι μια βασική μέθοδος της γραμμικής άλγεβρας μέσω της οποίας μετασχηματίζουμε μία ακολουθία γραμμικά ανεξάρτητων διανυσμάτων σε μία ακολουθία ορθοκανονικών γραμμικά ανεξάρτητων διανυσμάτων. Με αυτό τον τρόπο μπορούμε από μια οποιαδήποτε βάση ενός διανυσματικού χώρου να πάρουμε μία ορθοκανονική βάση, πράγμα πολύ χρήσιμο στις εφαρμογές. Στην εργασία αυτή όμως μας ενδιαφέρει να έχουμε ορθογώνια διανύσματα και έτσι παραλείπουμε την κανονικοποίηση. Για αυτό τον λόγο αναφέρουμε την μέθοδο ως ορθογωνοποίηση Gram-Schmidt.

Η μέθοδος έχει ως εξής:

Έστω μία ακολουθία διανυσμάτων $b_1, b_2, \ldots, b_n$. Εφαρμόζοντας σε αυτά την μέθοδο Gram-Schmidt παίρνουμε την ακολουθία $b_1^*, b_2^*, \ldots, b_n^*$ που συνδέεται με την αρχική με την σχέση:

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^* \text{ όπου } \mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad (1)$$

Καταρχήν παρατηρούμε ότι $\langle b_i^*, b_j^* \rangle = 0$ για κάθε i≠j.Ακόμα, span(b_1,b_2,..,b_n)=span(b_1^*,b_2^*,…,b_n^*). Επίσης, παρατηρούμε ότι αν τα b_i είναι ακέραια τότε τα b_i^* και τα μ_{ij} είναι ρητά.
Ξαναγράφοντας την (1) στην μορφή:

$$b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^* \text{ όπου } \mu_{ij} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad (2)$$

έχουμε:

$$\langle b_i, b_i^* \rangle = \langle b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*, b_i^* \rangle = \langle b_i^*, b_i^* \rangle$$

επομένως μπορούμε να ορίσουμε $\mu_{ij} = 1$ για i = j και $\mu_{ij} = 0$ για i>j.
Τότε η (2) γράφεται:

$$b_i = b_i^* + \sum_{j=1}^{i} \mu_{ij} b_j^*$$

ή σε μορφή πινάκων $B=B^*M^T$ όπου ο M^T είναι ο ανάστροφος του κάτω τριγωνικού πίνακα

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ \mu_{21} & 1 & 0 & \dots & 0 \\ \vdots & \mu_{32} & \ddots & & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ \mu_{n1} & \mu_{n2} & \mu_{n3} & \dots & 1 \end{bmatrix}$$

Παρατηρούμε εδώ ότι det(M)=1 αλλά ο M δεν είναι απαραίτητα ακέραιος πίνακας, *άρα γενικά δεν είναι unimodular*.

Αποδεικνύεται ότι η μέθοδος Gram-Schmidt είναι πολυωνυμικού χρόνου. Αυτό σημαίνει ότι μπορούμε από μία οποιαδήποτε βάση ενός διανυσματικού χώρου να υπολογίσουμε σε πολυωνυμικό χρόνο μία ορθοκανονική βάση του και είναι κάτι που θα μας χρειαστεί στη συνέχεια όταν θα δούμε άλλους αλγορίθμους που χρησιμοποιούν τη μέθοδο Gram-Schmidt.

Θα αναφέρουμε τώρα την ανισότητα Hadamard που θα μας χρειαστεί παρακάτω.

Ανισότητα Hadamard) Έστω $b_1,b_2,\dots,b_n$ διανύσματα του R^n (για τους σκοπούς μας αρκούσε να είναι ακέραια αλλά η ανισότητα ισχύει γενικότερα) που τα θεωρούμε ως γραμμές ενός πίνακα $B \in M_{n,n}(R)$. Τότε ισχύει $|\det(B)| \leq (\prod_{i=1}^{n} \|b_i\|_2)$.

Απόδειξη

Καταρχήν παρατηρούμε από την (2) ότι

$$\|b_i\|^2 = \|b_i^*\|^2 + \sum_{j=1}^{i} \mu_{ij}^2 \|b_j^*\|^2 \geq \|b_i^*\|^2 \Rightarrow \|b_i\| \geq \|b_i^*\|$$

με την ισότητα να ισχύει ανν $\mu_{ij} = 0$ για κάθε j.
Έχουμε $\det(B)^2 = \det(B^TB) = \det(MB^{*T}B^*M^T) = \det(M)\det(B^{*T}B^*)\det(M^T) = \prod_{i=1}^{n} \|b_i^*\|^2$ γιατί ο πίνακας $B^{*T}B^*$ είναι ένας nxn πίνακας με στοιχεία τα $\langle b_i^*, b_j^* \rangle$, τα οποία είναι μηδέν για i≠j και ίσα με $\|b_i^*\|^2$ για i=j, δηλαδή είναι ένας διαγώνιος πίνακας

με στοιχεία στην διαγώνιο τα $\|b_i^*\|^2$ επομένως η ορίζουσά του είναι ίση με $\prod_{i=1}^{n}\|b_i^*\|^2$

Από τα παραπάνω συνάγουμε ότι:

$|\det(B)|=\sqrt{\det(B^T B)} - \sqrt{\det(B^{*T} B^*)} - \prod_{i=1}^{n}\|b_i^*\| \leq \prod_{i=1}^{n}\|b_i\|$.

Ο λόγος $\frac{\prod_{i=1}^{n}\|b_i\|}{\det L}$ συμβολίζεται με δ(B) και λέγεται *έλλειμμα ορθογωνιότητας* του B, και μας δείχνει πόσο "κοντά" στον B^* (τον αντίστοιχο Gram-Schmidt) και συνεπώς πόσο κοντά είναι τα διανύσματα του B στο να είναι ορθογώνια. Ισχύει $\delta(B)\geq 1$ με την ισότητα να ισχύει αν τα διανύσματα της βάσης είναι ορθογώνια. Το αντίστροφο λέγεται *λόγος Hadamard (Hadamard ratio)* και συμβολίζεται H(B).Όσο πιο κοντά στο ένα είναι το H(B) τόσο πιο κοντά στο να είναι ορθογώνια είναι τα διανύσματα της βάσης.

3.3) Άλγεβρα

Θα αναφέρουμε μερικά στοιχεία από την άλγεβρα που θα χρειαστούν παρακάτω, ιδιαίτερα στο κρυπτοσύστημα NTRU.

Ορισμός 3.2) Έστω a,b ακέραιοι. Θα λέμε ότι ο a είναι ισότιμος με τον b modulo m αν η διαφορά τους a-b διαιρείται με τον m και γράφουμε $a\equiv b \pmod m$. Το m λέγεται και modulus.

Ισχύει η ακόλουθη πρόταση:

Πρόταση 3.3) Έστω $m\geq 1$ ακέραιος. Τότε:

I)Αν $a_1\equiv b_1 \pmod m$ και $a_2\equiv b_2 \pmod m$ τότε $a_1\pm a_2\equiv b_1\pm b_2 \pmod m$ και $a_1 a_2\equiv b_1 b_2 \pmod m$.

II)Αν a ακέραιος τότε $a\cdot b\equiv 1 \pmod m$ για κάποιο ακέραιο b αν και μόνο αν ΜΚΔ(a,m)=1. Αν το b υπάρχει τότε λέγεται πολλαπλασιαστικός αντίστροφος του a modulo m.

Για παράδειγμα, ας πάρουμε a=7 και m=15. Τότε ΜΚΔ(7,15)=1 και επομένως υπάρχει το $7^{-1} \bmod 15$ το οποίο είναι το 13.Πράγματι $7\cdot 13=91\equiv 1 \bmod 15$. Αν πάρουμε a=4,m=15 παρατηρούμε ότι ΜΚΔ(4,15)=1 και $4\cdot 4\equiv 1 \bmod 15$, δηλαδή το 4 έχει πολλαπλασιαστικό αντίστροφο mod 15 τον εαυτό του. Γνωρίζουμε ότι ένας ακέραιος a γράφεται ως $a=m\cdot q+r$ με $0\leq r<m$ άρα $a\equiv r \pmod m$ για κάποιον ακέραιο r μεταξύ 0 και m-1.Επομένως όταν δουλεύουμε με ακέραιους modulo m μπορούμε να χρησιμοποιήσουμε μόνο τους ακεραίους r με $0\leq r<m$. Συνεπώς ορίζουμε:

$Z/mZ = \{0,1,2,\ldots,m-1\}$ και ονομάζουμε το Z/mZ το δακτύλιο των ακεραίων modulo m. Παρατηρούμε από την άλγεβρα ότι το Z/mZ είναι ο δακτύλιος-πηλίκο του Z με το κύριο ιδεώδες mZ και οι αριθμοί $0,1,\ldots,m-1$ είναι αντιπρόσωποι των κλάσεων ισοδυναμίας που αποτελούν τα στοιχεία του Z/mZ. Ορίζουμε ακόμα το σύνολο $(Z/mZ)^*$ = {a ανήκει στο Z/mZ: ΜΚΔ (a,m)=1},δηλαδή το σύνολο των στοιχείων του Z/mZ που έχουν αντιστρόφους. Τα στοιχεία του Z/mZ που έχουν αντιστρόφους λέγονται μονάδες και το $(Z/mZ)^*$ λέγεται ομάδα των μονάδων modulo m. Σαν παράδειγμα αναφέρουμε την $(Z/7Z)^*=\{1,2,3,4,5,6\}$ και την $(Z/8Z)^*=\{1,3,5,7\}$.Παρατηρούμε ότι για m=7 (πρώτο) όλα τα στοιχεία εκτός από το 0 έχουν αντίστροφο. Αυτό ισχύει γενικότερα, δηλαδή για p πρώτο ισχύει $(Z/pZ)^*=\{1,2,\ldots,p-1\}$(αποδεικνύεται κατευθείαν από τον ορισμό του $(Z/mZ)^*$ και του γεγονότος ότι p πρώτος, άρα ΜΚΔ $(x,p)=1$ για $0<x<p$).Θα αναφερθούμε τώρα εκτενέστερα στους δακτυλίους. Καταρχήν δίνουμε τους ακόλουθους ορισμούς.

Ορισμός 3.4) Αντιμεταθετικός δακτύλιος με μοναδιαίο στοχείο πολλαπλασιασμού είναι ένα σύνολο R που το έχουμε εφοδιάσει με δύο πράξεις που συμβολίζουμε με + και * που ικανοποιούν τις ακόλουθες ιδιότητες:

Ιδιότητες της +

Ύπαρξης ουδέτερου στοιχείου	Υπάρχει το μηδενικό στοιχείο 0 ώστε 0+a=a+0 για κάθε a στο R
Αντιστροφής	Για κάθε στοιχείο a του R υπάρχει το προσθετικό αντίστροφο b τέτοιο ώστε a+b=b+a
Προσεταιριστική	(a+b)+c=a+(b+c) για όλα τα a,b,c στο R
Αντιμεταθετική	a+b=b+a για όλα τα a,b στο R

Με αυτές τις ιδιότητες το R είναι μία αντιμεταθετική ομάδα.

Ιδιότητες της *

Ύπαρξης ουδέτερου Στοιχείου	Υπάρχει το στοιχείο 1 στο R, τέτοιο ώστε 1*a=a*1=a για κάθε a στο R
Προσεταιριστική	(a*b)*c=a*(b*c) για όλα τα a,b,c στο R
Αντιμεταθετική	a*b=b*a για όλα τα a,b στο R

Το R μόνο με τις ιδιότητες αυτές είναι σχεδόν μια αντιμεταθετική ομάδα (λείπει η ύπαρξη αντίστροφου στοιχείου και έτσι δεν είναι ομάδα).

Ιδιότητα που συνδέει τις δύο πράξεις

	a*(b+c)=a*b+a*c για όλα τα a,b ,c στο R

Προφανώς αν αφαιρέσουμε την αντιμεταθετική ιδιότητα της * και την ύπαρξη του μοναδιαίου στοιχείου πολλαπλασιασμού (της πράξης *) παίρνουμε τον ορισμό του δακτυλίου (ring). Εμείς δώσαμε κατευθείαν αυτό τον ορισμό γιατί μας ενδιαφέρουν οι δακτύλιοι που έχουν αυτές τις ιδιότητες και μία ακόμα που φαίνεται στον ορισμό που ακολουθεί.

Ορισμός 3.5) Ένας αντιμεταθετικός δακτύλιος στον οποίο κάθε μη μηδενικό στοιχείο έχει πολλαπλασιαστικό αντίστροφο λέγεται **σώμα (field).**

Αναφέρουμε μερικά παραδείγματα (σαν + εννοούμε την γνωστή πρόσθεση)
1)R=Q,*=ο γνωστός πολλαπλασιασμός. Τότε το Q είναι προφανώς σώμα.
2)R=Z,*= ο γνωστός πολλαπλασιασμός. Τα μόνα στοιχεία του Z που έχουν πολλαπλασιαστικό αντίστροφο είναι το 1 και το -1 άρα το Z είναι αντιμεταθετικός δακτύλιος αλλά όχι σώμα.
3)R=Z/mZ,* ο γνωστός πολλαπλασιασμός και + η γνωστή πρόσθεση modulo m. Προφανώς είναι αντιμεταθετικός δακτύλιος με μοναδιαίο πολλαπλασιαστικό στοιχείο το 1. Μας ενδιαφέρει ιδιαίτερα η περίπτωση το m να είναι πρώτος δηλαδή να έχουμε R=Z/pZ. Τότε το R είναι σώμα (για το λόγο που αναφέραμε στο προηγούμενο παράδειγμα).Το R σε αυτή την περίπτωση συμβολίζεται και με F_p και λέγεται πεπερασμένο σώμα (επίσης συμβολίζεται και με GF(p) δηλαδή Galois

Field).Τα πεπερασμένα σώματα έχουν κεντρικό ρόλο στην σύγχρονη κρυπτογραφία. Στην εργασία αυτή θα χρησιμοποιούμε τους συμβολισμούς F_p και Z/mZ σαν να είναι το ίδιο .(Μπορούμε γιατί τα F_p και Z/mZ είναι ισόμορφα).
4)R=Z[x]={$a_0+a_1x+a_2x^2+\ldots+a_nx^n$:n≥0 και $a_0,a_1,a_2\ldots,a_n$ ακέραιοι},δηλαδή όλα τα πολυώνυμα με ακέραιους συντελεστές .Το R σε αυτή την περίπτωση καλείται πολυωνυμικός δακτύλιος. Αντί για Z μπορούμε να πάρουμε κάποιο πεπερασμένο σώμα, για παράδειγμα το F_3. Για παράδειγμα το $11+203x+155x^2$ είναι στοιχείο του Z[x] ενώ στον F_3[x] γράφεται $2+2x+2x^2$ (οι συντελεστές του πολυωνύμου στον F_3 είναι οι συντελεστές του πολυωνύμου στον Z[x] modulo 3).
Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι πολυωνυμικοί δακτύλιοι σε κάποιο σώμα γιατί συμπεριφέρονται όπως το Z, δηλαδή οι ιδιότητες του Z μεταφέρονται και σε αυτούς. Έτσι μπορούμε να κάνουμε πράξεις και να ορίσουμε διαιρέτες, αντιστρόφους κτλ όπως στους ακεραίους. Υπάρχει μάλιστα και ο εκτεταμένος ευκλείδειος αλγόριθμος για την εύρεση ΜΚΔ. Προχωρώντας ένα βήμα παραπέρα μπορούμε να ορίσουμε αυτό που πραγματικά μας ενδιαφέρει σε αυτή την εργασία, τους συνελικτικούς πολυωνυμικούς δακτύλιους πηλίκο (convolution quotient rings).
Ορισμός 3.6) Για N θετικό ακέραιο ο δακτύλιος των συνελικτικών πολυωνύμων τάξης N ορίζεται ως ο δακτύλιος πηλίκο R=$\frac{Z[x]}{x^{N-1}}$.Όμοια ο δακτύλιος των συνελικτικών πολυωνύμων τάξης N(modulo q) είναι ο δακτύλιος πηλίκο $R_q=\frac{(Z/qZ)[x]}{x^{N-1}}$. Αποδεικνύεται ότι κάθε στοιχείο του R ή του R_q έχει μοναδικό αντιπρόσωπο της μορφής $a_o+a_1x+\ldots+a_{N-1}x^{N-1}$ με συντελεστές στο Z ή στο (Z/qZ) αντίστοιχα. Στο a(x) μπορούμε να αντιστοιχήσουμε ένα διάνυσμα a με στοιχεία τους συντελεστές του a(x) δηλαδή $a=(a_0,a_1,\ldots,a_{N-1})\in Z^N$ και όμοια για το R_q. Έτσι, η πρόσθεση πολυωνύμων αντιστοιχεί σε πρόσθεση διανυσμάτων, ο πολλαπλασιασμός όμως αντιστοιχεί σε συνέλιξη διανυσμάτων. Έστω a(x),b(x) ∈ R τότε το γινόμενό τους δίνεται από τον τύπο a(x)*b(x)=c(x) με $c_k=\sum_{i+j\equiv k(mod\ n)} a_i\ b_{k-1}$. Για το R_q ισχύει το ίδιο μόνο που η c_k υπολογίζεται modulo q.Τέλος, ισχύει η ακόλουθη πρόταση που παρουσιάζουμε χωρίς απόδειξη.
Πρόταση 3.7) Έστω q πρώτος και a(x) ∈R_q. Το a(x) έχει πολλαπλασιαστικό αντίστροφο ανν ΜΚΔ(a(x),x^N-1)=1 στο (Z/qZ)[x].

3.4) Πλέγματα

Υπενθυμίζουμε ότι αν B={$b_1,b_2,\ldots,b_n$} γραμμικά ανεξάρτητα διανύσματα του $\Re^m$ το πλέγμα που παράγεται από τον B είναι το L{B}={$\sum_{i=1}^{n} x_i\cdot b_i : x_i\in Z$} ={B•x:x∈ Z} και το σύνολο B είναι μια βάση για το L(B).Στη δεύτερη περίπτωση θεωρούμε το B ως ένα πίνακα με στήλες τα $b_1,b_2,\ldots,b_n$ όχι απαραίτητα τετραγωνικό-αν $b_i\in\Re^n$ τότε $B\in\Re^{mxn}$).Τότε το n είναι ο βαθμός του πλέγματος (rank(L)=n) ενώ το m είναι η διάσταση του πλέγματος (dim(L)=m).Αν m=n τότε το πλέγμα λέγεται πλήρους διάστασης. Με τέτοια πλέγματα θα ασχοληθούμε κυρίως σε αυτήν την εργασία.

Ας παρατηρήσουμε εδώ ότι για έναν δεδομένο πίνακα B με γραμμικά ανεξάρτητες στήλες η διαφορά μεταξύ του πλέγματος που παράγεται από τον B και του διανυσματικού χώρου που παράγεται από τον B είναι ότι οι συντελεστές x_i των

διανυσμάτων είναι ακέραιοι στην πρώτη περίπτωση και πραγματικοί στην δεύτερη. Συνεπώς, το πλέγμα είναι ένα διακριτό σύνολο. Πιο γενικά ισχύει ότι: $L \subseteq \Re^m$ πλέγμα $\Leftrightarrow L$ διακριτή προσθετική υποομάδα του $\Re^m$.

Η έννοια της βάσης ενός πλέγματος παίζει κεντρικό ρόλο για τις εφαρμογές που θα αναπτύξουμε στη συνέχεια για αυτό θα την μελετήσουμε διεξοδικότερα. Παρατηρούμε καταρχήν ότι αν B είναι μια βάση για το L(B) θα είναι και για το γραμμικό χώρο που παράγεται από το span(B).Το αντίστροφο δεν ισχύει πάντοτε. Για παράδειγμα, η 2B είναι βάση για το span(B) αλλά όχι για το L(B) γιατί οι συντελεστές των b_i που προκύπτουν δεν είναι ακέραιοι. Μας ενδιαφέρει τώρα να δούμε πότε δύο βάσεις B και B΄ παράγουν το ίδιο πλέγμα.

Θεώρημα 3.8)Δύο βάσεις B και B΄ παράγουν το ίδιο πλέγμα αν και μόνο αν υπάρχει unimodular πίνακας U τέτοιος ώστε B=B΄U.

Απόδειξη

Υπενθυμίζουμε ότι ένας unimodular πίνακας είναι ένας τετραγωνικός πίνακας με ακέραια στοιχεία και ορίζουσα ίση με +1 ή -1.

΄Εστω λοιπόν ότι υπάρχει ένας unimodular U τέτοιος ώστε B=B΄U. Θα δείξουμε ότι L(B)=L(B΄).Πράγματι το B=B΄U γράφεται $B΄=BU^{-1}$ όπου U^{-1} ο αντίστροφος του U. Από τις δύο αυτές σχέσεις παρατηρούμε ότι $L(B)\subseteq L(B΄)$ και παρόμοια $L(B΄)\subseteq L(B)$ επομένως L(B)=L(B΄).

Αντίστροφα, έστω B,B΄ δύο βάσεις του ίδιου πλέγματος L(B)=L(B΄), επομένως μπορούμε να εκφράσουμε τα στοιχεία της μίας βάσει της άλλης. Άρα, υπάρχουν ακέραιοι τετραγωνικοί πίνακες T και T΄ τέτοιοι ώστε B=B΄T΄ και B΄=BT. Από τις δύο αυτές εξισώσεις παίρνουμε B=BTT΄ ή ισοδύναμα B(I-TT΄)=0. Αφού όμως τα στοιχεία της βάσης είναι γραμμικά ανεξάρτητα πρέπει I-TT΄=0 ή TT΄=I. Δηλαδή det(TT΄)=det(I)=1. Συνεπώς det(T)×det(T΄)=1 και αφού T,T΄ ακέραιοι, $\det(T),\det(T΄) \in \mathbb{Z}$ πρέπει $\det(T)=\det(T΄)=\pm 1$.

Από το θεώρημα αυτό συμπεραίνουμε ότι εφαρμόζοντας τις παρακάτω πράξεις επί
γραμμών πίνακα σε μία βάση παίρνουμε μία νέα βάση για το ίδιο πλέγμα:

- Πολλαπλασιασμός μιας στήλης με -1
- Εναλλαγή δύο στηλών
- Πολλαπλασιασμός μιας στήλης με έναν ακέραιο αριθμό και πρόσθεση σε άλλη στήλη

Παρατηρούμε ότι η εφαρμογή των πράξεων αυτών ισοδυναμεί με πολλαπλασιασμό
από δεξιά με έναν unimodular πίνακα και άρα δεν αλλάζει το πλέγμα που παράγει η βάση.

Ένα ακόμα σημαντικό χαρακτηριστικό ενός πλέγματος είναι η ορίζουσά του.

Ορισμός 3.9) Η ορίζουσα ενός πλέγματος L συμβολίζεται με detL και ορίζεται ως: $detL = (\det[\langle b_i, b_j \rangle_{1 \le i,j \le n}])^{\frac{1}{2}}$. Αυτός ο ορισμός είναι γενικός και ισχύει για όλα τα πλέγματα. Τα $\langle b_i, b_j \rangle$ μπορούμε να τα φανταστούμε ως τα στοιχεία ενός nxn πίνακα A, δηλαδή $A_{ij}= \langle b_i, b_j \rangle$ (οι αγκύλες υποδηλώνουν το εσωτερικό γινόμενο και αυτός ο πίνακας λέγεται πίνακας Gram). Αν περιοριστούμε στο σύνηθες εσωτερικό γινόμενο τότε ο ορισμός παίρνει την μορφή: $detL = \sqrt{\det(B^T B)}$.

Αν επιπλέον περιοριστούμε σε πλέγματα πλήρους βαθμού (δηλαδή m=n) ο B είναι τετραγωνικός πίνακας και έτσι παίρνουμε detL=|detB|. Εκτός και αν αναφέρουμε διαφορετικά αυτός θα είναι ο ορισμός που θα χρησιμοποιήσουμε σε αυτή την εργασία. Από την ανισότητα Hadamard παίρνουμε : $detL \le \prod_{i=1}^{n} \|b_i\|$.

Παρουσιάζουμε τώρα ένα βασικό θεώρημα:

Θεώρημα 3.10)Η ορίζουσα ενός πλέγματος είναι ανεξάρτητη από τη βάση του

Απόδειξη

Πράγματι, έστω B και C δύο διαφορετικές βάσεις του ίδιου πλέγματος L δηλαδή L(B)=L(C). Τότε υπάρχει unimodular πίνακας U τέτοιος ώστε B=CU. Έχουμε λοιπόν $(detL)=\det(B^TB)^{1/2}=\det(U^TC^TCU)^{1/2}=\det(C^TC)^{1/2}$ επειδή det(U)=1.

Από αυτό το θεώρημα συμπεραίνουμε ότι η ορίζουσα είναι μια αναλλοίωτη του πλέγματος. Ακόμα, βλέπουμε ότι δύο βάσεις B και C είναι ισοδύναμες αν |det(B)|=|det(C)| (το αντίστροφο γενικά δεν ισχύει) .

Για να εξετάσουμε την έννοια της ορίζουσας γεωμετρικά θα δώσουμε πρώτα τον ακόλουθο ορισμό:

Ορισμός 3.11) Έστω $B=[b_1,b_2,..,b_n] \in \mathbb{R}^{m \times n}$ μια βάση, τότε ορίζουμε ως το θεμελιώδες παραλληλεπίπεδο ή βασικό μπλοκ της B και συμβολίζουμε με F(B) το σύνολο των σημείων : $F(B) = \{\sum_{i=1}^{n} x_i b_i : 0 \le x < 1\}$

Από τον ορισμό βλέπουμε ότι το F(B) είναι ημιανοικτό, άρα για $v \in L(B)$ το F(B)+v δημιουργεί μία διαμέριση όλου του $\mathbb{R}^n$. Είναι προφανές ότι η επιλογή της βάσης καθορίζει το θεμελιώδες παραλληλεπίπεδο που θα πάρουμε. Όμως ο όγκος του παραλληλεπιπέδου είναι ανεξάρτητος από την επιλογή της βάσης. Πράγματι, αν με B^* συμβολίσουμε την βάση που παίρνουμε από την B εφαρμόζοντας την μέθοδο Gram-Schmidt τότε $vol(F(B))= \prod_{i=1}^{n} \|b_i^*\| = detL$.

Ένας εναλλακτικός ορισμός για την ορίζουσα είναι: detL(B)=vol(F(B)).Δηλαδή η ορίζουσα είναι ο όγκος του θεμελιώδους παραλληλεπιπέδου.

Γεωμετρικά, η σχέση του θεμελιώδους παραλληλεπιπέδου και του πλέγματος δίνεται από το ακόλουθο θεώρημα.

Θεώρημα 3.12)Έστω L ένα πλέγμα βαθμού n και $b_1,b_2,..,b_n$ n ανεξάρτητα διανύσματα του πλέγματος. Τα διανύσματα αυτά αποτελούν μία βάση του πλέγματος ανν $F(b_1,b_2,..,b_n) \cap L=\{0\}$.

Απόδειξη

Έστω ότι τα $b_1,b_2,..,b_n$ είναι μια βάση του L. Τότε εξ'ορισμού το μεν L είναι το σύνολο όλων των ακέραιων γραμμικών συνδυασμών τους, το δε $F(b_1,b_2,..,b_n)$ είναι το σύνολο όλων των γραμμικών συνδυασμών τους με συντελεστές που ανήκουν

στο διάστημα [0,1). Προφανώς ο μόνος ακέραιος συνδυασμός που ανήκει στο F είναι αυτός που οι συντελεστές είναι 0 και άρα η τομή των F και L είναι το {0}.

Έστω τώρα, αντίστροφα, ότι $F(b_1,b_2,..,b_n) \cap L = \{0\}$. Θεωρούμε ένα διάνυσμα x $\in$ L το οποίο γράφεται ως $x = \sum y_i b_i$ (γιατί τα b_i είναι γραμμικά ανεξάρτητα) για κάποια $y_i \in R$ και έστω $z = \sum(y_i - \lfloor y_i \rfloor)b_i$. Τότε το z ανήκει στο πλέγμα (γιατί το πλέγμα είναι κλειστό όσον αφορά την πρόσθεση) και επιπλέον ανήκει και στο $P(b_1,b_2,..,b_n)$ γιατί $(y_i - \lfloor y_i \rfloor \in [0,1)$.

Άρα, z=0 και αφού τα b_i είναι γραμμικά ανεξάρτητα παίρνουμε $y_i = \lfloor y_i \rfloor \forall\, y_i \in \mathbb{R}$.

Δηλαδή πήραμε ένα τυχαίο διάνυσμα του πλέγματος και δείξαμε ότι μπορεί να εκφραστεί σαν ακέραιος συνδυασμός των b_i,επομένως τα $b_1,b_2,..,b_n$ αποτελούν μία βάση του L. ■

Πρόταση 3.13) Έστω $L \subseteq R^n$ ένα πλέγμα και F ένα θεμελιώδες παραλληλεπίπεδο για το L. Τότε κάθε w $\in$ στο R^n μπορεί να γραφτεί στην μορφή w=t+v για μοναδικό v$\in$ L και μοναδικό t$\in$ F.

Απόδειξη

Έστω $v_1,v_2,\ldots,v_n$ μία βάση του L που δίνει το F. Τότε τα $v_1,v_2,\ldots,v_n$ είναι γραμμικά ανεξάρτητα στο R^n , δηλαδή είναι μια βάση του R^n. Επομένως $w=a_1v_1+a_2v_2+\ldots+a_nv_n$ για κάποια $a_1,\ldots,a_n \in R$. Όμως $a_i= t_i+s_i$ με $0\leq t_i<1$ και $s_i \in$

Z. Άρα $w= (t_1v_1+\ldots+t_nv_n)+(s_1v_1+\ldots+s_nv_n)$ όπου ο προσθετέος με τα t_i είναι ένα διάνυσμα t που ανήκει στο P ενώ ο προσθετέος με τα s_i είναι ένα διάνυσμα v που ανήκει στο L, δηλαδή w=t+v.

Θα δείξουμε τώρα ότι αυτή η αναπαράσταση είναι μοναδική. Έστω ότι το w έχει δύο αναπαραστάσεις δηλαδή w = t + v = t`+v`. Τότε $(t_1+s_1)v_1+\ldots+(t_n+s_n)v_n = (t_1`+s_1`)v_1+\ldots+(t_n`+s_n`)v_n$. Αφού τα v_i είναι γραμμικά ανεξάρτητα έχουμε $t_i+s_i=t_i`+s_i`$ δηλαδή $t_i-t_i`=s_i'-s_i \in Z$. Αλλά τα $t_i,t_i`$ είναι μικρότερα του 1 και επομένως για να είναι το $t_i-t_i`$ ακέραιος πρέπει $t_i=t_i`$. Επομένως η αναπαράσταση του w είναι μοναδική.

Θα δώσουμε τώρα τον ορισμό του υποπλέγματος.

Ορισμός 3.14) Έστω L_1,L_2 πλέγματα του ίδιου βαθμού με $L_1 \subseteq L_2$. Τότε λέμε ότι το L_1 είναι υποπλέγμα του L_2. Αποδεικνύεται ότι για κάθε βάση $a_1,a_2,..,a_n$ του L_1 υπάρχει μία βάση του L_2 έστω $b_1,b_2,..b_n$ τέτοια ώστε $[a_1,a_2,..,a_n]=[b_1,b_2,..b_n]T$, όπου T ένας άνω τριγωνικός πίνακας που ανήκει $M_{n,n}(Z)$ και ότι ισχύει και το αντίστροφο.

Δίνουμε μερικά παραδείγματα:

A) Έστω το πλέγμα $L=\{(x_o,x_1,x_2,\ldots,x_n) \in Z^{n+1} \mid \sum_{i=0}^{n} x_i = 0\}$. Μία βάση του δίνεται από τα ακόλουθα διανύσματα-γραμμές:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} -1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & -1 & 1 & 0 \\ 0 & \cdots & 0 & 0 & -1 & 1 \end{bmatrix}$$

Το πλέγμα που παράγεται από τα διανύσματα αυτά δηλαδή το $L_1(b_1,b_2,..b_n)$ είναι ένα υποπλέγμα του L αφού τα $b_1,b_2,..b_n$ ανήκουν στο L και είναι γραμμικά ανεξάρτητα.

Β) Έστω το πλέγμα L={ $x_o,x_1,x_2,\ldots,x_n) \in Z^{n+1} \mid \sum_{i=0}^{n} x_i \equiv 0 \ (mod\ 2)$}. Μία βάση του δίνεται από τα ακόλουθα διανύσματα-γραμμές:

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_{n-1} \\ b_n \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 & 0 & \cdots & 0 \\ 1 & -1 & 0 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \cdots & 0 & 1 & -1 & 0 \\ 0 & \cdots & 0 & 0 & 1 & -1 \end{bmatrix}$$

Γ) Το $Z^n = \{(x_1,x_2,\ldots,x_n): x_1,x_2,\ldots,x_n \in Z\}$ είναι το πλέγμα που αποτελείται από όλα τα διανύσματα με ακέραιες συντεταγμένες.

Δ)Έστω το πλέγμα L που παράγεται από τα διανύσματα $v_1=(2,1,3)$, $v_2=(1,2,0)$, $v_3=(2,-3,-5)$. Θέτοντας τα ως αντίστοιχες γραμμές παίρνουμε τον πίνακα $A=\begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{pmatrix}$. Έστω τώρα τρία νέα διανύσματα του πλέγματος που παράγονται από τις σχέσεις $w_1=v_1+v_3$, $w_2=v_1-v_2+2v_3$, $w_3= v_1+2v_2$

Αυτό ισοδυναμεί με τον πολλαπλασιασμό του A από αριστερά με τον $U=\begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$. Επομένως τα w_1,w_2,w_3 είναι οι γραμμές του πίνακα $B=UA=\begin{pmatrix} 4 & -2 & -2 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{pmatrix}$. Παρατηρούμε ότι det(U)=-1 άρα τα w_1,w_2,w_3 αποτελούν και αυτά μία βάση του L. Ο αντίστροφος του U είναι $U^{-1}=\begin{pmatrix} 4 & -2 & -1 \\ -2 & 1 & 1 \\ -3 & 2 & 1 \end{pmatrix}$ και οι γραμμές του μας δείχνουν πώς να εκφράσουμε τα v_i μέσω των w_j, δηλαδή $v_1=4w_1-2w_2-w_3$, $v_2=-2w_1+w_2+w_3$, $v_3=-3w_1+2w_2+w_3$.

Τέλος detL=|det(A)|=36=|det(B)|.

3.5)Το θεώρημα Minkowski και τα διαδοχικά ελάχιστα

Μέχρι τώρα είδαμε ότι ένα πλέγμα μπορεί να έχει πολλές διαφορετικές βάσεις, που όμως όλες έχουν την ίδια ορίζουσα. Παράλληλα, μπορούμε να διαλέξουμε μία βάση με διανύσματα σχεδόν ορθογώνια. Ενδιαφερόμαστε όμως να έχουμε και όσο το δυνατόν "μικρότερα" διανύσματα, όπου η έννοια του "μικρότερου" προφανώς εξαρτάται από την νόρμα που χρησιμοποιούμε. Στην ενότητα αυτή θα δώσουμε την έννοια των διαδοχικών ελαχίστων και επίσης, ένα άνω φράγμα για το "μικρότερο" διάνυσμα σε ένα πλέγμα.

Ορίζουμε καταρχήν ως το μικρότερο διάνυσμα ενός πλέγματος αυτό το οποίο είναι μη μηδενικό και η νόρμα του είναι η μικρότερη δυνατή, δηλαδή αν u είναι διάνυσμα ενός πλέγματος L, διάφορο του 0, τότε το u είναι το μικρότερο αν $||u|| \leq ||w||$ για κάθε w του L. Προφανώς λοιπόν ανάλογα με τη νόρμα μπορούμε να έχουμε διαφορετικά μικρότερα διανύσματα. Σαν παράδειγμα έστω το πλέγμα που παράγεται από τα διανύσματα $b_1=[1,1]^T$ και $b_2=[0,2]^T$, τότε το $[0,2]^T$ είναι το μικρότερο διάνυσμα (όχι όμως και το μοναδικό, υπάρχει και το $[2,0]^T$) για την ℓ_1

όχι όμως και για την ℓ_2 ή την ℓ_∞ (σε αυτή την περίπτωση το $[1,1]^T$ είναι μικρότερο).
Δίνουμε τώρα τον ακόλουθο ορισμό.

Ορισμός 3.15) Διαδοχικά ελάχιστα $\lambda_1,\lambda_2,...,\lambda_v$ (successive minima)
Έστω ||.|| μία οποιαδήποτε νόρμα. Για κάθε πλέγμα $L \subseteq R^m$ τάξης n τα διαδοχικά ελάχιστα $\lambda_1,\lambda_2,...,\lambda_v$ με βάση την ||.|| ορίζονται ως:
$\lambda_i=\lambda_i(L)=\inf\{r>0|$υπάρχουν i γραμμικά ανεξάρτητα διανύσματα $c_1,c_2,...,c_i$ στο L με $||c_j||\leq r$ για κάθε $j=1,2,\ldots,i\}$ για $i=1,2,\ldots,n$.

Με άλλα λόγια το λ_1 είναι η νόρμα του μικρότερου μη μηδενικού διανύσματος του L, το λ_2 η νόρμα του μικρότερου μη μηδενικού διανύσματος του L που είναι γραμμικά ανεξάρτητο του λ_1 , το λ_3 είναι η νόρμα του μικρότερου μη μηδενικού διανύσματος του L που είναι γραμμικά ανεξάρτητο των λ_1 και λ_2 και ούτω καθεξής. Από τον ορισμό έχουμε ότι $\lambda_1\leq\lambda_2\leq\ldots\leq\lambda_v$.
Δίνουμε τώρα τους ακόλουθους ορισμούς:
Για κάθε a στο R^n και για οποιοδήποτε r>0 η κλειστή σφαίρα (μπάλα) ακτίνας r με κέντρο το a είναι το σύνολο $B_r(a)=\{x$ στο $R^n : ||x-a||\leq r\}$.
Έστω S ένα υποσύνολο του R^n , τότε το S είναι
α) φραγμένο, αν υπάρχει $B_r(0)$ για κάποιο κατάλληλο r τέτοιο ώστε $S\subseteq B_r(0)$
β) συμμετρικό, αν για κάθε x στο S το –x ανήκει και αυτό στο S
γ)κυρτό, αν για οποιαδήποτε x,y στο S και t στο [0,1] το tx+(1-t)y ανήκει στο S (δηλαδή αν για οποιαδήποτε δύο σημεία του S ανήκει στο S και η ευθεία που τα ενώνει)
δ)κλειστό, αν για a στο R^n τέτοιο ώστε κάθε $B_r(a)$ να περιέχει ένα σημείο του S, το a να ανήκει στο S.
ε)συμπαγές , αν είναι κλειστό και φραγμένο
Με βάση τους παραπάνω ορισμούς παρουσιάζουμε το ακόλουθο σημαντικό θεώρημα.

Θεώρημα 3.16) (Θεώρημα του Minkowski) Έστω $L\subseteq R^n$ πλέγμα διάστασης n και $S\subseteq R^n$ ένα συμμετρικό κυρτό σύνολο για το οποίο ισχύει $Vol(S)>2^n det(L)$. Τότε το S περιέχει ένα μη μηδενικό διάνυσμα του πλέγματος L.
Αν το S είναι κλειστό τότε αρκεί να πάρουμε $Vol(S)\geq 2^n det(L)$.

Απόδειξη

Έστω F ένα θεμελιώδες παραλληλεπίπεδο του L. Έχουμε αποδείξει ότι κάθε διάνυσμα a στο S μπορεί να γραφεί μοναδικά στη μορφή $a=v_a+w_a$ με $v_a \in L$ και $w_a \in F$. Θεωρούμε τώρα το σύνολο $\frac{1}{2}S=\{\frac{1}{2}a: a \in S\}$ και την απεικόνιση $\frac{1}{2}S\rightarrow F$, δηλαδή $\frac{1}{2}a\rightarrow w_{1/2a}$. Όμως $Vol(\frac{1}{2}S)=\frac{1}{2^n}Vol(S)>det(L)=Vol(F)$ από υπόθεση. Παρατηρούμε ότι επειδή το S είναι φραγμένο η απεικόνιση διατηρεί τον όγκο. Επομένως αφού ο όγκος του $\frac{1}{2}S$ είναι αυστηρά μεγαλύτερος του όγκου του F τότε υπάρχουν δύο διαφορετικά σημεία $\frac{1}{2}a_1$ και $\frac{1}{2}a_2$ στο S που έχουν την ίδια εικόνα w στο F. Άρα βρήκαμε δύο διαφορετικά σημεία στο S τέτοια ώστε $\frac{1}{2}a_1= v_1+w$ και $\frac{1}{2}a_2= v_2+w$. Παίρνοντας τη διαφορά έχουμε $\frac{1}{2}a_1-\frac{1}{2}a_2=v_1-v_2 \in L$. Επειδή το S είναι συμμετρικό το $-a_2 \in S$ και επειδή είναι κυρτό το $\frac{1}{2}a_1+(-\frac{1}{2}a_2) \in S$. Επομένως $v_1-v_2 \in S\cap L$ και $v_1-v_2\neq 0$, δηλαδή βρήκαμε ένα μη μηδενικό κυρτό διάνυσμα του L στο S.

Υποθέτουμε τώρα ότι το S είναι κλειστό και Vol(S)=2^ndet(L). Για κάθε k≥1 θεωρούμε το σύνολο (1+$\frac{1}{k}$) S και εφαρμόζουμε το προηγούμενο αποτέλεσμα για να βρούμε ένα μη μηδενικό διάνυσμα v_k που ανήκει στο (1+$\frac{1}{k}$) S∩L. Παρατηρούμε ότι $\cap_{k=1}^{\infty}\left(1+\frac{1}{k}\right)S = S$ γιατί το S είναι κλειστό, Ακόμα, τα v_k ανήκουν στο φραγμένο σύνολο 2S και επειδή το L είναι διακριτό και το πλήθος των v_k είναι πεπερασμένο. Άρα καθώς το k τείνει στο άπειρο ένα μη μηδενικό διάνυσμα v (που είναι κάποιο από τα v_k) θα επαναλαμβάνεται άπειρες φορές. Έτσι παίρνοντας αυτό το διάνυσμα και με βάση την παρατήρηση που κάναμε έχουμε ότι 0≠v ∈ S∩L που είναι αυτό που θέλαμε να αποδείξουμε.

Το θεώρημα του Minkowski μας επιτρέπει να αποδείξουμε το ακόλουθο πολύ σημαντικό θεώρημα που οφείλεται στον Hermite.

Θεώρημα 3.17) (Θεώρημα του Hermite) Κάθε πλέγμα L διάστασης n περιέχει ένα μη μηδενικό διάνυσμα v ∈ L τέτοιο ώστε $\|v\| \leq \sqrt{n}\det(L)^{\frac{1}{n}}$

Απόδειξη

Έστω L⊂R^n ένα πλέγμα και S ένας υπερκύβος (δηλαδή ένας κύβος σε n διαστάσεις) με κέντρο το 0 και πλευρές μήκους 2B, δηλαδή
S={(x_1,…,x_n) ∈ R^n : -B≤x_i≤B για όλα τα i , 1≤i≤n}. Το S είναι συμμετρικό, κλειστό και φραγμένο με όγκο Vol(S)=$(2B)^n$. Θέτοντας B=$\det(L)^{\frac{1}{n}}$ παίρνουμε Vol(S)=2^ndet(L) και από το θεώρημα του Minkowski έχουμε ότι υπάρχει διάνυσμα v=(v_1,v_2,…,v_n) τέτοιο ώστε 0≠v∈ S∩L. Άρα $\|v\| = \sqrt{(v_1^2 + v_2^2 + \cdots v_n^2)} \leq \sqrt{n}B = \sqrt{n}\det(L)^{\frac{1}{n}}$.

Το θεώρημα αυτό μας εξασφαλίζει την ύπαρξη ενός "μικρού" διανύσματος (όχι υποχρεωτικά του μικρότερου) και μάλιστα το μέγεθος του εξαρτάται από την διάσταση και την ορίζουσα του πλέγματος. Θα μας ενδιέφερε να έχουμε μια εκτίμηση του v για δεδομένη διάσταση για οποιοδήποτε πλέγμα L. Αυτό μας δίνει η σταθερά του Hermite . Για δεδομένη διάσταση n η σταθερά του Hermite γ_n είναι η μικρότερη τιμή για την οποία κάθε πλέγμα L διάστασης n περιέχει ένα μη μηδενικό διάνυσμα v που ικανοποιεί την σχέση: $\|v\|^2$=$\gamma_n$det(L)$^{2/n}$. Προφανώς $\gamma_n \leq n$. Για μεγάλα n ισχύει $\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e}$.

Στην απόδειξη του θεωρήματος Hermite εφαρμόσαμε το θεώρημα Minkowski σε έναν υπερκύβο. Μπορούμε να έχουμε καλύτερη προσέγγιση αν εφαρμόσουμε το θεώρημα σε μία υπερσφαίρα (σφαίρα σε n διαστάσεις) για μεγάλα n, που είναι επίσης κλειστό, συμμετρικό και φραγμένο σύνολο. Καταρχήν αναφέρουμε κάποια αποτελέσματα από την ανάλυση για τον όγκο μιας σφαίρας και στη συνέχεια εφαρμόζουμε το θεώρημα Minkoswki για την υπερσφαίρα.

Ορισμός 3.18) Η συνάρτηση γάμμα ορίζεται για s>0 από το ολοκλήρωμα $\Gamma(s) = \int_0^{\infty} t^s e^{-t}\frac{1}{t}dt$. Αναφέρουμε μερικές βασικές ιδιότητες χωρίς απόδειξη.

α) Το ολοκλήρωμα συγκλίνει για όλα τα s>0.

β) Γ(1)=1 και Γ(s+1)=sΓ(s). Έτσι ορίζεται αναδρομικά για τα s του (α) αλλά και για αρνητικά μη ακέραια s.

γ) Για n ακέραιο με n≥1, Γ(n+1)=n!

δ) $\Gamma(1/2)=\sqrt{\pi}$

Ο τύπος του Stirling λέει ότι $\ln\Gamma(s+1)=\ln(s/e)^s+\frac{1}{2}\ln(2\pi s)+O(1)$ καθώς το s τείνει στο άπειρο, ή πιο απλά για μεγάλα s $(\Gamma(s+1))^{1/s}\approx\frac{s}{e}$.

Η γάμμα συνάρτηση μας χρειάζεται για τον υπολογισμό του όγκου της σφαίρας. Πράγματι αποδεικνύεται ότι αν $B_r(a)$ μία σφαίρα ακτίνας r στο R^n, τότε ο όγκος της δίνεται από τον τύπο $\mathrm{Vol}(B_r(a))=\frac{\pi^{n/2}r^n}{\Gamma(1+\frac{n}{2})}$.

Επομένως έχουμε $(\mathrm{Vol}(B_r(a)))^{1/n}=\frac{\pi^{1/2}r}{\Gamma(1+\frac{n}{2})^{1/n}}\approx\frac{\pi^{1/2}r}{(n/2e)^{1/2}}=\sqrt{\frac{2\pi e}{n}}r$ όπου χρησιμοποιήσαμε τον τύπο του Stirling.

Εφαρμόζοντας το θεώρημα Minkowski για τη σφαίρα $B_r(0)$ έχουμε ότι διαλέγοντας r τέτοιο ώστε $\mathrm{Vol}(B_r(0))\geq 2^n\det(L)^{1/n}$ δηλαδή $\sqrt{\frac{2\pi e}{n}}r\geq 2\det(L)^{1/n}\rightarrow r\geq\sqrt{\frac{2n}{\pi e}}\det(L)^{1/n}$ κατά προσέγγιση και υπάρχει ένα μη μηδενικό διάνυσμα $v\in L$ που περιέχεται στη σφαίρα και για το οποίο ισχύει $\|v\|\leq r$. Επομένως, παίρνοντας r τέτοιο ώστε $r\cong\sqrt{\frac{2n}{\pi e}}\det(L)^{1/n}$ έχουμε ότι $\|v\|\leq\sqrt{\frac{2n}{\pi e}}\det(L)^{1/n}$ κατά προσέγγιση. Έτσι έχουμε μια βελτίωση της τάξης του $\sqrt{\frac{2}{\pi e}}\cong 0.484$. Επομένως έχουμε ότι $\lambda_1(L)\leq\sqrt{\frac{2n}{\pi e}}\det(L)^{1/n}$.

Ο ανωτέρω τύπος μας δίνει ένα άνω φράγμα για το $\lambda_1(L)$ όταν το n είναι μεγάλο. Θα ασχοληθούμε τώρα με το ακόλουθο ερώτημα. Αν έχουμε ένα τυχαίο πλέγμα L ποιο είναι το αναμενόμενο μήκος του $\lambda_1(L)$;

Ορισμός 3.19) Έστω L ένα πλέγμα διάστασης n. Το κατά Γκάους αναμενόμενο μικρότερο μήκος (Gaussian expected shortest length) ορίζεται ως $\sigma(L)=\sqrt{\frac{n}{2\pi e}}(detL)^{\frac{1}{n}}$. Για το σ(L) ισχύει $\|v_{min}\|\approx\sigma(L)$, όπου v_{min} το διάνυσμα του L με το μικρότερο μήκος.

Ο υπολογισμός του σ(L) βασίζεται σε ένα ευριστικό επιχείρημα που θα αναλύσουμε κατωτέρω.

Έστω μια σφαίρα B_r και F το θεμελιώδες παραλληλεπίπεδο του L. Τότε κατά προσέγγιση ο αριθμός των θεμελιωδών παραλληλεπιπέδων που περιέχονται στη σφαίρα ισούται με τον όγκο της σφαίρας δια του όγκου του θεμελιώδους παραλλεπιπέδου, δηλαδή $\#\{F\}\approx\frac{Vol(B_r)}{Vol(F)}=\frac{Vol(B_r)}{\det L}$. Διαλέγοντας r τέτοιο ώστε $\mathrm{Vol}(B_r)\approx\det L$ η σφαίρα ακτίνας r με κέντρο το t θα περιέχει άλλο ένα σημείο του L (εκτός του t). Για μεγάλα n αντικαθιστώντας τον τύπο που δίνει τον όγκο της σφαίρας παίρνουμε $(\frac{2\pi e}{n})^{\frac{n}{2}}r^n\approx detL$ οπότε λύνοντας ως προς r παίρνουμε το σ(L). Παρατηρούμε ότι ο τύπος που δώσαμε ισχύει για μεγάλα n. Για μικρά n αν

αντικαταστήσουμε τον τύπο για τον όγκο της σφαίρας παίρνουμε $\sigma(L)=\frac{1}{\sqrt{\pi}}(\Gamma(1+n/2)\det(L)^{\frac{1}{n}}$.

Παίρνοντας n= 6 και υπολογίζοντας το σ(L) και με τον πρώτο τύπο παίρνουμε $\sigma(L)=0.5927\det(L)^{1/6}$ ενώ με τον δεύτερο παίρνουμε $\sigma(L)=0.7605\det(L)^{1/n}$ δηλαδή έχουμε σημαντική διαφορά. Αντίστοιχα, για n=100 έχουμε $\sigma(L)=2.420\det(L)^{1/100}$ με τον πρώτο τύπο και $\sigma(L)=2.490\det(L)^{1/100}$ με τον δεύτερο, δηλαδή ασήμαντη διαφορά.

Με τον ίδιο τρόπο αν w είναι ένα τυχαίο διάνυσμα τότε περιμένουμε το $v \in L$ να ικανοποιεί τη σχέση $\|v-w\| \approx \sigma(L)$.

Είναι εμπειρικά διαπιστωμένο το γεγονός ότι αν το $\lambda_1(L)$ είναι σημαντικά μικρότερο του σ(L) τότε οι αλγόριθμοι αναγωγής πλέγματος όπως ο LLL βρίσκουν πιο εύκολα (δηλαδή με λιγότερους υπολογισμούς) το $\lambda_1(L)$.

3.6) Ο αλγόριθμος πλησιέστερης κορυφής του Babai

Ένας τρόπος για να επιλύσουμε το CVP παρουσιάστηκε από τον Babai με αυτό τον αλγόριθμο. Η κεντρική ιδέα είναι η εξής: έστω L ένα πλέγμα, $\{v_1,v_2,\ldots,v_n\}$ μια βάση του, και F το θεμελιώδες παραλληλεπίπεδο. Παρατηρούμε ότι μεταφέροντας το F με τα στοιχεία του L μπορούμε να καλύψουμε όλο το R^n, δηλαδή ένα τυχαίο w $\in R^n$ είναι μια μοναδική μεταφορά F+v του F από ένα τυχαίο διάνυσμα $v \in L$. Συνεπώς, μπορούμε να προσεγγίσουμε το w (το οποίο δεν ανήκει απαραίτητα στο L) με την πλησιέστερη κορυφή στο w του παραλληλεπιπέδου F+v. Για να βρούμε την πλησιέστερη κορυφή παρατηρούμε ότι $w=v+a_1v_1+a_2v_2+\ldots+a_nv_n$ με τα a_i πραγματικούς αριθμούς μεταξύ 0 και 1. Επομένως θέτοντας ίσο με μηδέν όποιο a_i είναι μικρότερο του ½ και ίσο με 1 όποιο είναι μεγαλύτερο από ή ίσο με με ½ παίρνουμε την πλησιέστερη κορυφή. Έτσι λοιπόν έχουμε:

Θεώρημα 3.20) (Ο αλγόριθμος πλησιέστερης κορυφής του Babai)

Έστω $L \subseteq R^n$ ένα πλέγμα με βάση $\{v_1,v_2,\ldots,v_n\}$ και έστω $w \in R^n$ ένα τυχαίο διάνυσμα. Ο ακόλουθος αλγόριθμος επιλύει το CVP :

Γράψε το $w=b_1v_1+b_2v_2+\ldots+b_nv_n$ με $b_1,b_2,\ldots,b_n \in R$.

Θέσε a_i= ΑκέραιοΜέρος(b_i) αν b_i- ΑκέραιοΜέρος(b_i) < ½ αλλιώς a_i= ΑκέραιοΜέρος(b_i)+1 (αυτό το συμβολίζουμε με a_i=round(b_i))

Επέστρεψε το διάνυσμα $v=a_1v_1+a_2v_2+\ldots+a_nv_n$.

Παρατηρούμε ότι το v είναι αναγκαστικά μια προσέγγιση για το w. Το πόσο καλή είναι εξαρτάται από τη βάση που θα χρησιμοποιήσουμε. Αν τα διανύσματα της βάσης είναι σχεδόν ορθογώνια μεταξύ τους τότε ο αλγόριθμος μας δίνει μια πολύ καλή προσέγγιση. Αντίθετα , αν τα διανύσματα της βάσης σε μεγάλο βαθμό μη ορθογώνια (δηλαδή το έλλειμα ορθογωνιότητας πλησιάζει το 1 ή αλλιώς ο λόγος Hadamard πλησιάζει το 0) τότε ο αλγόριθμος αποτυγχάνει. Για αυτό το λόγο στην πράξη τον εφαρμόζουμε σε μια βάση όπου ήδη έχουμε εφαρμόσει τον αλγόριθμο LLL ώστε η βάση να είναι "καλή". Δίνουμε ένα μικρό παράδειγμα.

Παράδειγμα Αλγόριθμου Babai)

Έστω $L \subseteq R^2$ με διανύσματα βάσης $v_1=(137,212)$ και $v_2=(215,-187)$ και $w=(53172,81743)$ το τυχαίο διάνυσμα που θέλουμε να προσεγγίσουμε. Εφαρμόζουμε τον αλγόριθμο. Έτσι γράφουμε το w σαν γραμμικό συνδυασμό των v_1,v_2. Έχουμε λοιπόν $w=t_1v_1+t_2v_2$ δηλαδή

$53172=137t_1+215t_2$ και $81743=312t_1-187t_2$. Λύνοντας το σύστημα παίρνουμε $t_1\approx296.85$ και $t_2\approx58.15$.

Σύμφωνα με το δεύτερο βήμα στρογγυλοποιούμε τα t_1 και t_2 στους πλησιέστερους ακεραίους δηλαδή $a_1= 297$ και $a_2=58$

Το διάνυσμα που ζητάμε είναι το $v=a_1v_1+a_2v_2 = 297(137,312)+58(215,-187)= (53159,81818)$. Ακόμα $\|v-w\|\approx76.12$ που είναι μικρή απόσταση. Ας υπολογίσουμε τώρα το λόγο Hadamard. Έχουμε

$H(v_1,v_2)=\left(\frac{\det(L)}{\|v_1\|\|v_2\|}\right)^{1/2}=\left(\frac{92699}{(340.75)(284.95)}\right)^{1/2} \approx 0.977$ που είναι πολύ κοντά στο 1. Δηλαδή η βάση είναι σχεδόν ορθογώνια.

Ας θεωρήσουμε μια καινούρια βάση $z_1=5v_1+6v_2$ και $z_2=19v_1+23v_2$ (παρατηρούμε ότι η ορίζουσα του πίνακα αλλαγής βάσης $\begin{pmatrix} 5 & 6 \\ 19 & 23 \end{pmatrix}$είναι 1 άρα η νέα βάση είναι ισοδύναμη με την παλιά). Εφαρμόζοντας πάλι τον αλγόριθμο του Babai παίρνουμε $z= (56405,82444)$ και $\|z-w\|\approx3308.12$ δηλαδή η απόστασή τους είναι μεγάλη. Αν υπολογίσουμε το λόγο Hadamard αυτής της βάσης παίρνουμε $H(z_1,z_2)\approx0.077$ δηλαδή η βάση είναι μη ορθογώνια και ο αλγόριθμος αποτυγχάνει.

Κεφάλαιο 4) Ο αλγόριθμος LLL

Όπως έχουμε αναφέρει σε πολλές εφαρμογές μας ενδιαφέρει τα διανύσματα της βάσης ενός πλέγματος να είναι μικρού μήκους και όσο γίνεται πιο κοντά στο να είναι ορθογώνια μεταξύ τους. Η διαδικασία με την οποία από μία βάση βρίσκουμε μία άλλη με διανύσματα που να έχουν τα χαρακτηριστικά που προαναφέραμε λέγεται αναγωγή πλέγματος (lattice reduction) και η βάση που παίρνουμε από τη διαδικασία αυτή λέγεται ανηγμένη (reduced). Η πιο γνωστή διαδικασία βασίζεται στον αλγόριθμο LLL, από τους Lenstra, Lenstra και Lovàsz και δημοσιεύτηκε στο Mathematische Annalen 261 (1982),σελίδες 515-534. Ο LLL είναι ένας προσεγγιστικός πολυωνυμικός αλγόριθμος με λόγο προσέγγισης C^n όπου C μικρή σταθερά και n η διάσταση του πλέγματος. Έτσι για πλέγματα μικρής διάστασης ο αλγόριθμος αποδίδει εξαιρετικά αλλά όσο μεγαλώνει η διάσταση η απόδοση πέφτει. Αυτό σημαίνει ότι κρυπτοσυστήματα που βασίζονται σε πλέγματα είναι ασφαλή για μεγάλα n.

4.1)Αναγωγή κατά Gauss

Ξεκινάμε με ένα αλγόριθμο του Gauss που εφαρμόζεται με επιτυχία σε πλέγματα διάστασης 2. Αν και δεν είναι αποδοτικός για μεγαλύτερες διαστάσεις τον εξετάζουμε σαν εισαγωγή για τον αλγόριθμο LLL που θα μελετήσουμε στην επόμενη παράγραφο γιατί μοιράζονται κάποιες ιδέες που φαίνονται καλύτερα στις δύο διαστάσεις. Η βασική ιδέα είναι η αφαίρεση πολλαπλάσιου του μικρότερου διανύσματος βάσης από το μεγαλύτερο μέχρι να φτάσουμε στο σημείο που περαιτέρω αφαίρεση είναι αδύνατη με βάση τα κριτήρια που έχουμε θέσει. Έτσι έχουμε τον ακόλουθο ορισμό:

Ορισμός 4.1) Ανηγμένη βάση κατά Gauss

Μια βάση λέγεται ανηγμένη κατά Gauss αν για τα διανύσματά της b_1,b_2 ισχύει $||b_1||,||b_2|| \leq ||b_1-b_2||,||b_1+b_2||$.

Ορισμός 4.1.2) Καλά διατεταγμένη βάση

Μια βάση λέγεται καλά διατεταγμένη αν $||b_1|| \leq ||b_1-b_2|| < ||b_2||$

Για να κάνουμε την αφαίρεση θα μας βόλευε να χρησιμοποιούσαμε τον τύπο από την ορθοκανονικοποίηση Gram-Schmidt. Όμως το διάνυσμα που προκύπτει δεν είναι ακέραιος και άρα δεν ανήκει στο L. Για αυτό το λόγο παίρνουμε τον τύπο στρογγυλοποιημένο (όπως στον αλγόριθμο του Babai) για να είναι ακέραιος.
Δίνουμε τώρα τον αλγόριθμο του Gauss (ισχύει για τη νόρμα l_2):

Αλγόριθμος 4.3) Αλγόριθμος Αναγωγής κατά Γκάους στις δύο διαστάσεις
Αν $||v_1|| < ||v_2||$ αντάλλαξε τα v_1 και v_2
$m=\text{round}((v_1v_2)/||v_1||^2)$
Αν $m=0$ τότε επέστρεψε τα v_1 και v_2
Αλλιώς αντικατέστησε το v_2 με το v_2-mv_1
Επανέλαβε

Παρατηρούμε ότι αν m=0 συνεπάγεται ότι $((v_1v_2)/||v_1||^2)\leq ½$. Αν ο αλγόριθμος δεν τερμάτιζε τα διανύσματα που θα επέστρεφε θα γίνονταν όλο και μικρότερα · όμως επειδή ο αριθμός των διανυσμάτων που είναι μικρότερος από τα αρχικά είναι πεπερασμένος κάποια στιγμή τα διανύσματα δεν μπορούν να γίνουν μικρότερα και άρα ο αλγόριθμος τερματίζει. Θα δείξουμε τώρα ότι ο αλγόριθμος όντως επιστρέφει το μικρότερο διάνυσμα (δεν είναι υποχρεωτικό να είναι μοναδικό).
Πράγματι έστω v_1,v_2 τα διανύσματα που επιστρέφει ο αλγόριθμος με v_1 το μικρότερο, δηλαδή $||v_1||\leq||v_2||$. Έστω τώρα ένα τυχαίο $v \in L$ με $v=a_1v_1+a_2v_2$, τα a_1,a_2 ακέραιοι. Τότε $||v||^2= ||a_1v_1+a_2v_2||^2=a_1^2||v_1||^2+2a_1a_2(v_1v_2)+a_2^2||v_2||^2\geq a_1^2||v_1||^2 - 2a_1a_2|v_1v_2|+a_2^2||v_2||^2\geq a_1^2||v_1||^2-|a_1a_2|||v_1||^2+a_2^2||v_2||^2$ (από την παρατήρηση και το ότι το v_1 είναι μικρότερο από το $||v_2||$) $= (a_1^2-|a_1||a_2|+a_2^2)||v_1||^2$. Όμως η ποσότητα $x_1^2-x_1x_2+x_2^2 = (x_1-½\ x_2)^2+3/4x_2^2$ είναι πάντα θετική εκτός αν $x_1=x_2=0$ που στην περίπτωσή μας δεν ισχύει γιατί τότε το v θα ήταν το μηδενικό διάνυσμα. Άρα $||v||^2\geq||v_1||^2$ και επομένως το v_1 είναι το μικρότερο μη μηδενικό διάνυσμα στο L.
Δίνουμε ένα μικρό παράδειγμα :
Παράδειγμα) Αλγόριθμος Gauss

Έστω $v_1=(31,59)$ και $v_2=(37,70)$. Έχουμε $||v_1||\leq||v_2||$ οπότε υπολογίζουμε το $m=round((v_1v_2)/||v_1||^2)=round(5277/4442)=round(1.1880)=1$. Επομένως η νέα βάση είναι $v_1^1=v_1=(31,59)$ και $v_2^1=v_2-mv_1=(6,11)$.Τελειώσαμε το πρώτο βήμα και επαναλαμβάνουμε. Τώρα $||v_1^1||=66.68$ και $||v_2^1||=12.53$ οπότε τα ανταλλάσουμε και έχουμε $v_1^2=(6,11)$ και $v_2^2=(31,59)$. Υπολογίζουμε το m κατά τα γνωστά και βγαίνει m=5.Έτσι βρίσκουμε τα διανύσματα (6,11) και (31,59)-5*(6,11)=(1,4).Θέτουμε $v_1^3=(1,4)$ και $v_2^3=(6,11)$. Το m=3 οπότε παίρνουμε $v_1^4=(3,-1)$ και $v_2^4=(1,4)$. Τώρα m=0 άρα βρήκαμε την ανηγμένη κατά Gauss βάση (3,-1) και (1,4) με το (3,-1) να είναι ένα μικρότερο μη μηδενικό διάνυσμα στο L.Παρατηρούμε ότι αν ορίσουμε κατά τα γνωστά τον $A=(v_1,v_2)=\begin{pmatrix}3 & -1\\ 1 & 4\end{pmatrix}$ και τον πολλαπλασιάσουμε από αριστερά με τον $U=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}$, με det(U)=-1, παίρνουμε $B=UA=\begin{pmatrix}-3 & 1\\ 1 & 4\end{pmatrix}$ και για το $b_1=(-3,1)$ ισχύει $||b_1||=||v_1||$.

Ο αλγόριθμος του Gauss μπορεί να γενικευτεί για οποιαδήποτε νόρμα. Η κεντρική ιδέα παραμένει ίδια όμως η αρχική βάση πρέπει να είναι καλά διατεταγμένη και το m να επιλέγεται έτσι ώστε $m \in Z$ και η ποσότητα $||v_2-mv_1||$ να είναι ελάχιστη για τη νόρμα που χρησιμοποιούμε.

4.2) Ο αλγόριθμος LLL

Ξεκινάμε την περιγραφή του αλγόριθμου LLL αναφέροντας τι θέλουμε να πετύχουμε: από μία βάση $\{v_1,v_2,\ldots,v_n\}$ ενός πλέγματος L να πάρουμε μία καλύτερη βάση. Με το καλύτερη εννοούμε τα διανύσματα να είναι όσο το δυνατόν μικρότερα, ξεκινώντας μάλιστα από το μικρότερο. Ακόμα θέλουμε τα διανύσματα της βάσης που θα πάρουμε να είναι όσο το δυνατόν πιο κάθετα το ένα με το άλλο δηλαδή τα εσωτερικά γινόμενα v_iv_j να είναι όσο γίνεται πιο κοντά στο μηδέν. Από την ανισότητα του Hadamard έχουμε $detL=Vol(F)\leq||v_1||\ ||v_2||\ \ldots||v_n||$, όπου F είναι το θεμελιώδες παραλληλεπίπεδο του L. Όσο πιο κοντά στο να είναι ορθογώνια είναι η βάση τόσο η ανισότητα πλησιάζει την ισότητα.

Όπως και με τον αλγόριθμο του Gauss ξεκινάμε από την ορθοκανονικοποίηση Gram-Schmidt κάνοντας κάποιες στρογγυλοποιήσεις για να καταλήξουμε σε μια καλύτερη βάση, σύμφωνα με κάποια κριτήρια που έχουμε θέσει. Έτσι έχουμε $v_1^*=v_1$ και για i≥2 θέτουμε $v_i^*=v_i-\sum_{j=1}^{i-1}\mu_{i,j}v_j^*$ με $\mu_{i,j}=\frac{v_i v_j^*}{\|v_j^*\|^2}$ για 1≤j≤i-1. Με αυτή τη διαδικασία παίρνουμε μια ορθογώνια βάση $B^*=\{v_1^*,v_2^*,\ldots,v_n^*\}$ για το διανυσματικό χώρο που παράγεται από την $B=\{v_1,v_2,\ldots,v_n\}$ αλλά όχι για το πλέγμα L γιατί τα $\mu_{i,j}$ δεν είναι υποχρεωτικά ακέραια άρα και τα v_i^* που προκύπτουν δεν είναι ακέραια και το ίδιο και οι γραμμικοί συνδυασμοί τους με ακέραιους συντελεστές. Όπως θα δείξουμε όμως με την ακόλουθη πρόταση οι δύο βάσεις έχουν την ίδια ορίζουσα.

Πρόταση 4.4) Έστω $B=\{v_1,v_2,\ldots,v_n\}$ μια βάση για το πλέγμα L και έστω $B^*=\{v_1^*,v_2^*,\ldots,v_n^*\}$ η βάση που προκύπτει εφαρμόζοντας τη μέθοδο Gram-Schmidt.Τότε $detL=\prod_{i=1}^{n}\|v_i^*\|$.

Απόδειξη

Έστω $F=F(v_1,v_2,\ldots,v_n)$ ο πίνακας που έχει γραμμές τις συντεταγμένες των $v_1,v_2,\ldots,v_n$. Ισχύει det(L)=|det(F)|. Όμοια παίρνουμε και τον $F^*=F(v_1^*,v_2^*,\ldots,v_n^*)$. Από τον τύπο της κανονικοποίησης προκύπτει ότι $F=MF^*$ όπου M ο πίνακας αλλαγής βάσης $M=\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 & 0 \\ \mu_{2,1} & 1 & 0 & \ldots & 0 & 0 \\ \mu_{3,1} & \mu_{3,2} & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & & \vdots \\ \mu_{n-1,1} & \mu_{n-1,2} & \mu_{n-1,3} & \ldots & 1 & 0 \\ \mu_{n,1} & \mu_{n,2} & \mu_{n,3} & \ldots & \mu_{n,n-1} & 1 \end{pmatrix}$

Ο M είναι κάτω τριγωνικός πίνακας με όλα τα στοιχεία της κύριας διαγωνίου ίσα με 1, επομένως det(M)=1. Επομένως $det(L)=|det(F)|=|det(MF^*)|=|det(M)(det(F^*)|=|det(F^*)|=\prod_{i=1}^{n}\|v_i^*\|$ (επειδή τα v_i^* είναι αναμεταξύ τους κάθετα).

Διαισθητικά, η ιδέα πίσω από τη μέθοδο Gram-Schmidt είναι η εξής:

v_i^*= προβολή του v_i στη θήκη $(v_1,v_2,..v_{i-1})^{\perp}$ όπου με $\perp$ συμβολίζουμε το ορθογώνιο συμπλήρωμα. Θα εφαρμόσουμε την ίδια ιδέα τροποποιημένη ώστε να παίρνουμε κατάλληλους συντελεστές για τον ορισμό της ανηγμένης LLL βάσης.

Ορισμός 4.5) LLL ανηγμένη βάση (LLL reduced basis)

Έστω $B=\{v_1,v_2,\ldots,v_n\}$ μια βάση για ένα πλέγμα L και $B^*=\{v_1^*,v_2^*,\ldots,v_n^*\}$ η αντίστοιχη βάση που παράγεται από τη διαδικασία Gram-Schmidt. Η βάση B λέγεται LLL ανηγμένη αν ικανοποιεί τις ακόλουθες δύο προϋποθέσεις:

1) Συνθήκη Μεγέθους $|\mu_{i,j}|=\frac{v_i v_j^*}{\|v_j^*\|^2}\leq\frac{1}{2}$ για όλα τα 1≤j<i≤n
2) Συνθήκη Lovász $\|v_i^*\|^2\geq(\frac{3}{4}-\mu_{i,i-1}^2)\|v_{i-1}^*\|^2$ για όλα τα 1≤j<i≤n

Η συνθήκη Lovász γράφεται και ως $\left\|v_i^* + \mu_{i,i-1}v_{i-1}^*\right\|^2 \geq \frac{3}{4}\|v_{i-1}^*\|^2$ γιατί τα v_i^* και v_{i-1}^* είναι εκ κατασκευής ορθογώνια.
Η συνθήκη Lovász διαισθητικά σημαίνει ότι ||προβολή του v_i στη θήκη $(v_1,v_2,\ldots,v_{i-2})^{\perp}$||≥3/4||προβολή του v_{i-1} στην θήκη $(v_1,v_2,\ldots,v_{i-2})^{\perp}$||
Αντί για το 3/4 πιο γενικά έχουμε παράμετρο δ με 1/4≤δ≤1. Στην πράξη όμως χρησιμοποιείται η τιμή ¾ και αυτή θα χρησιμοποιούμε σε αυτή την εργασία.
Το ακόλουθο θεώρημα μας λέει ότι η βάση που είναι LLL ανηγμένη είναι μια καλή βάση δηλαδή προσεγγίζει τα κριτήρια που θέσαμε στην αρχή της παραγράφου.

Θεώρημα 4.6) Έστω L ένα πλέγμα διάστασης n. Οποιαδήποτε LLL ανηγμένη βάση $\{v_1,v_2,\ldots,v_n)$ του L ικανοποιεί τις ακόλουθες δύο ιδιότητες:

1) $\prod_{i=1}^{n}\|v_i\| \leq 2^{n(n-1)/4}detL$
2) $\|v_j\| \leq 2^{(i-1)/2}\|v_i^*\|$ για όλα τα 1≤j<i≤n

Ακόμα το πρώτο διάνυσμα σε μια LLL ανηγμένη βάση ικανοποιεί τις σχέσεις

$$\|v_1\| \leq 2^{\frac{n-1}{4}}|detL|^{\frac{1}{n}} \kappa\alpha\iota \|v_1\| \leq 2^{\frac{n-1}{2}}\lambda_1(L)$$

Επομένως το πρώτο διάνυσμα μιας LLL ανηγμένης βάσης επιλύει το apprSVP με λόγο προσέγγισης $2^{(n-1)/2}$.

Απόδειξη

Από τη συνθήκη Lovász και το ότι $|\mu_{i,j}|\leq \frac{1}{2}$ παίρνουμε τη σχέση
$\|v_i^*\|^2 \geq \frac{1}{2}\|v_{i-1}^*\|^2$ ή $\|v_{i-1}^*\|^2 \leq 2\|v_i^*\|^2$ που αν τη εφαρμόσουμε επανηλλειμένα μέχρι κάποιο j, j<i, παίρνουμε την πολύ χρήσιμη σχέση

$$\left\|v_j^*\right\|^2 \leq 2^{i-j}\|v_i^*\|^2 \ (1)$$

Από τον τύπο της μεθόδου Gram-Schmidt έχουμε ότι
$\|v_i\|^2 = \left\|v_i^* + \sum_{j=1}^{i}\mu_{i,j}v_j^*\right\|^2 = \|v_i^*\|^2 + \sum_{j=1}^{i}\mu_{i,j}\left\|v_j^*\right\|^2$ (λόγω ορθογωνιότητας),
$\leq \|v_i^*\|^2 + \sum_{j=1}^{i}\frac{1}{4}\left\|v_j^*\right\|^2$ γιατί $\mu_{i,j}|\leq \frac{1}{2}$,
$\leq \|v_i^*\|^2 + \sum_{j=1}^{i}2^{i-j-2}\left\|v_j^*\right\|^2$ από την (1)
$= \frac{1+2^{i-1}}{2}\left\|v_j^*\right\|^2 \leq 2^{i-1}\left\|v_j^*\right\|^2$ αφού $1\leq 2^{i-1}$ για όλα τα i≥1 (2)
Πολλαπλασιάζοντας την (2) με τον εαυτό της για 1≤i≤n παίρνουμε
$\prod_{i=1}^{n}\|v_i\|^2 \leq \prod_{i=1}^{n}2^{i-1}\left\|v_j^*\right\|^2 = 2^{n(n-1)/2}\prod_{i=1}^{n}\left\|v_j^*\right\|^2 = 2^{n(n-1)/2}(detL)^2$ από την Πρόταση 4.2.1.Παίρνοντας τετραγωνικές ρίζες καταλήγουμε στην ιδιότητα 1.
Από τις (1) και (2) έχουμε
$\left\|v_j\right\|^2 \leq 2^{i-1}\left\|v_j^*\right\|^2 \leq 2^{j-1}2^{i-j}\|v_i^*\|^2 = 2^{i-1}\|v_i^*\|^2$ οπότε παίρνοντας τετραγωνικές ρίζες καταλήγουμε στην ιδιότητα 2.
Αν στην ιδιότητα 2 θέσουμε j=1 και πολλαπλασιάσουμε για 1≤i≤n παίρνουμε
$\|v_i\|^n \leq \prod_{i=1}^{n}2^{(i-1)/2}\left\|v_j^*\right\| = 2^{n(n-1)/4}\prod_{i=1}^{n}\left\|v_j^*\right\|^2 = 2^{n(n-1)/4}detL$ από την Πρόταση 4.4. Παίρνοντας ν-οστές ρίζες και θέτοντας όπου i το 1 προκύπτει η πρώτη σχέση για το v_1.
Για την τελευταία θεωρούμε ένα διάνυσμα ν στο L,διάφορο του μηδέν, το οποίο γράφεται

$v = \sum_{j=1}^{i} a_j v_i = \sum_{j=1}^{i} b_j v_j^*$ με $a_i \neq 0$ (το i είναι ο μεγαλύτερος δείκτης για τον οποίο το a_i είναι διάφορο του μηδενός, δηλαδή $a_j=0$ για j>i) και $a_{1,..,}$ a_i ακέραιους και $b_1,\ldots,b_i$ πραγματικούς. Επομένως $|a_i|\geq 1$.
Παρατηρούμε ότι $v \cdot v_i^* = a_i v_i v_i^* = b_i v_i^* \cdot v_i^* \; και \; v_i v_i^* = v_i^* \cdot v_i^*$
Επομένως $a_i = b_i$ και άρα $|b_i|\geq 1$.
Άρα $\|v\|^2 = \sum_{j=1}^{i} b_j^2 \left\|v_j^*\right\|^2 \geq b_i^2 \|v_i^*\|^2 \geq \|v_i^*\|^2 \geq 2^{-(i-1)}\|v_1\|^2 \geq 2^{-(n-1)}\|v_1\|^2$
Επομένως $\|v_1\| \leq 2^{(n-1)/2}\|v\|$
Αφού το v μπορεί να είναι οποιοδήποτε διάνυσμα του L διαλέγουμε $v=\lambda_1(L)$ οπότε καταλήγουμε στην σχέση που θέλουμε.

Δίνουμε τώρα τον αλγόριθμο LLL.

Αλγόριθμος 4.7) LLL

1) Είσοδος μια βάση $\{v_1,v_2,\ldots,v_n\}$ του L
2) Θέσε k=2
3) Θέσε $v_1^*=v_1$
4) Μέχρι k≤n επανέλαβε
5) Για j=1,2,3,…,k-1 επανέλαβε
6) Θέσε $v_k=v_k-\text{round}(\mu_{i,j})v_j^*$ (Αναγωγή μεγέθους)
7) Τέλος j βρόχου
8) Αν $\|\|v_k^*\|^2 \geq (\frac{3}{4} - \mu_{k,k-1}^2)\|v_{k-1}^*\|^2$ (Συνθήκη Lovász)
9) Θέσε k=k+1
10) Αλλιώς
11) Αντάλλαξε το v_{k-1} με το v_k (Βήμα Ανταλλαγής)
12) Θέσε k=max(k-1,2)
13) Τέλος Αν
14) Τέλος k βρόχου
15) Επέστρεψε ανηγμένη LLL βάση $\{v_1,v_2,\ldots,v_n\}$

Σε κάθε βήμα του αλγορίθμου $v_1^*,v_2^*,\ldots,v_k^*$ είναι τα ορθογώνια διανύσματα που παίρνουμε εφαρμόζοντας την διαδικασία Gram-Schmidt στα τρέχοντα $v_1,v_2,\ldots,v_k$ και $|\mu_{i,j}|=\frac{v_i v_j^*}{\left\|v_j^*\right\|^2}$.

Ο αλγόριθμος αφού πάρει σαν είσοδο μία βάση, σχηματίζει σε στάδια (k είναι το στάδιο) μια καινούρια (που τα διανύσματα είναι με αύξουσα σειρά μεγέθους, έτσι ώστε το πρώτο είναι το μικρότερο) , που ικανοποιεί την συνθήκη μεγέθους για τις LLL ανηγμένες βάσεις . Στη συνέχεια ελέγχει αν η καινούρια βάση ικανοποιεί τη συνθήκη Lovász . Αν ναι, προχωράει στο επόμενο στάδιο, αλλιώς αλλάζει τη σειρά των διανυσμάτων και επαναλαμβάνει από το προηγούμενο στάδιο. Υποθέτοντας ότι είμαστε στο στάδιο k ($1\leq k\leq n$) ,συμβολίζουμε με L_l το υποπλέγμα του L που παράγεται από τα $v_1,v_2,..,v_l$. Ο αλγόριθμος LLL σε κάθε πέρασμα αλλάζει τα υποπλέγματα L_l προσπαθώντας να βρει την κατάλληλη σειρά των διανυσμάτων βάσης (σε συνδυασμό με την αναγωγή μεγέθους) που ελαχιστοποιεί τις $\det(L_l)$ (με αύξουσα σειρά μεγέθους). Επειδή σε κάθε επανάληψη το k μπορεί είτε να μειωθεί είτε να αυξηθεί δεν είναι φανερό ότι ο αλγόριθμος τερματίζει. Θα δείξουμε όμως

ότι το Βήμα Ανταλλαγής εκτελείται πεπερασμένο αριθμό φορών, επομένως τελικά το k τελικά ικανοποιεί τη συνθήκη τερματισμού του k βρόχου.

Θεώρημα 4.8) Αλγόριθμος LLL
Έστω $\{v_1,v_2,\ldots,v_n\}$ μία βάση ενός πλέγματος L. Ο αλγόριθμος LLL τερματίζει μετά από πεπερασμένο αριθμό επαναλήψεων και επιστρέφει μια LLL ανηγμένη βάση στο L, σε πολυωνυμικό χρόνο. Μάλιστα, αν $B=\max\|v_i\|$ τότε ο αλγόριθμος εκτελεί τον k βρόχο $O(n^2\log n+n^2\log B)$ φορές.

Απόδειξη

Υποθέτουμε ότι ο αλγόριθμος τερματίζει. Τότε προφανώς μας δίνει μια LLL ανηγμένη βάση αφού τα βήματα [5]-[7] εξασφαλίζουν ότι πληρείται η συνθήκη μεγέθους ενώ το ότι k=n+1 στο τέλος σημαίνει ότι όλα τα διανύσματα ικανοποιούν την (βήμα [8]).
Θα δείξουμε ότι ο αλγόριθμος τερματίζει στην περίπτωση $L \subset Z$. Ορίζουμε τις ποσότητες

$$d_l = \prod_{i=1}^{l} \left\|v_j^*\right\|^2 \; και \; D = \prod_{l=1}^{n} d_l = \prod_{i=1}^{n} \left\|v_j^*\right\|^{2(n+1-i)}$$

Ισχύει $(detL_l)^2=d_l$.
Όταν εκτελούμε το βήμα [11],δηλαδή όταν έχουμε ανταλλαγή η τιμή του d_{k-1} και επομένως και του D αλλάζει. Αν l<k-1 τότε το d_l δεν περιλαμβάνει τα v_{k-1}^* και v_k^* που ανταλλάσσονται ενώ αν l≥k το d_l περιλαμβάνει και τα δύο άρα δεν επηρεάζεται από την ανταλλαγή. Επειδή για να γίνει ανταλλαγή πρέπει η συνθήκη Lovász να μην ικανοποιείται έχουμε ότι

$$\|\|v_k^*\|^2 \leq (\frac{3}{4} - \mu_{k,k-1}^2)\|v_{k-1}^*\|^2 \leq \frac{3}{4}\|v_{k-1}^*\|^2$$

Θα υπολογίσουμε πόσο επηρεάζει η ανταλλαγή το d_{k-1}. Συμβολίζουμε με d_{k-1}' την τιμή του d_{k-1} μετά την ανταλλαγή. Επομένως έχουμε

$$d_{k-1}' = \|v_1^*\|^2 \cdot \|v_2^*\|^2 \cdots \|v_{k-2}^*\|^2 \cdot \|v_k^*\|^2$$

$$= \|v_1^*\|^2 \cdot \|v_2^*\|^2 \cdots \|v_{k-2}^*\|^2 \cdot \|v_{k-1}^*\|^2 \cdot \frac{\|v_k^*\|^2}{\|v_{k-1}^*\|^2} = d_{k-1} \cdot \frac{\|v_k^*\|^2}{\|v_{k-1}^*\|^2} \leq \frac{3}{4} d_{k-1}$$

Η σχέση αυτή μας λέει ότι αν γίνει ανταλλαγή το d_{k-1}' ελαττώνεται κατά ένα παράγοντα $\frac{3}{4}$ τουλάχιστον.
Άρα, αν το βήμα [11] εκτελεστεί N φορές, η τιμή του D που είναι το γινόμενο των d_l ελαττώνεται κατά ένα παράγοντα $\left(\frac{3}{4}\right)^N$ τουλάχιστον.
Από το θεώρημα του Hermite έχουμε ότι

$$1 \leq min_{0\neq w\in L_l}\|w\| \leq \sqrt{l}(detL_l)^{\frac{1}{l}} \Rightarrow l^{\frac{-l}{2}} \leq detL_l$$

$$και \; επειδή \; d_l = (detL_l)^2 \; παίρνουμε \; d_l \geq l^{-l}$$ οπότε πολλαπλασιάζοντας για όλα τα l βρίσκουμε

$$D = \prod_{l=1}^{n} d_l \geq \prod_{l=1}^{n} l^{-l} \geq \prod_{l=1}^{n} l^{-n} = (n!)^{-n} \geq n^{-n^2} \; (επειδή \; n! \leq n^n$$

Επομένως το D έχει σαν κάτω φράγμα μία σταθερά που εξαρτάται από τη διάσταση του πλέγματος, άρα δεν μπορεί να μικρύνει απεριόριστα. Επομένως μπορεί να πολλαπλασιαστεί επί ¾ πεπερασμένο αριθμό φορών άρα ο αλγόριθμος τερματίζει.
Θα υπολογίσουμε τώρα ένα άνω φράγμα για τον αριθμό εκτελέσεων του k βρόχου (βήματα [4] μέχρι [14]) που είναι το κύριο μέρος του αλγορίθμου.

Έστω $D_{αρχ}$ η τιμή του D για την αρχική βάση και $D_{τελ}$ η τιμή του D για την τελική βάση (αυτή που μας δίνει ο αλγόριθμος όταν τερματίζει), N ο αριθμός των φορών που εκτελείται το βήμα [11] (τότε ο k βρόχος εκτελείται το πολύ 2N+n φορές).Σύμφωνα με όσα αναφέραμε παραπάνω ισχύει ότι

$n^{-n^2} \leq D_{τελ} \leq \left(\frac{3}{4}\right)^N D_{αρχ} \xrightarrow{παίρνοντας\ log}$

$N=O(n^2 logn+logD_{αρχ})$ (γιατί $log(3/4)<1$).
Επομένως αρκεί να υπολογίσουμε ένα φράγμα για το $D_{αρχ.}$ Από τη μέθοδο Gram Schmidt έχουμε ότι $\|v_i^*\| \leq \|v_i\|$ άρα

$D_{αρχ} = \prod_{i=1}^{n} \|v_i^*\|^{(n+1-i)} \leq \prod_{i=1}^{n} \|v_i\|^{n+1-i} \leq (max_{1\leq i\leq n}\|v_i\|)^{2(1+2+\cdots+n)} = B^{n^2+n}$.

Συνεπώς, $log(Dαρχ)=O(n^2 logB)$ και αυτό ολοκληρώνει την απόδειξη.

Αντί να μετρήσουμε τον αριθμό των φορών που εκτελείται ο κύριος βρόχος του αλγορίθμου μπορούμε να υπολογίσουμε τον αριθμό των βασικών αριθμητικών πράξεων που εκτελεί ο LLL, δηλαδή πόσες φορές εκτελείται ο εσωτερικός j βρόχος και πόσες πράξεις εκτελούνται στις συντεταγμένες κάθε διανύσματος. Για παράδειγμα η πρόσθεση δύο διανυσμάτων και ο πολλαπλασιασμός βαθμωτού με διάνυσμα έχουν κόστος n βασικές αριθμητικές πράξεις. Με αυτό τον τρόπο μέτρησης αποδεικνύεται στο άρθρο που δημοσιεύτηκε ο LLL ότι τερματίζει μετά από $O(n^6(logB)^3)$ βασικές αριθμητικές πράξεις.

Παράδειγμα για τον αλγόριθμο LLL)

Έστω ένα πλέγμα L έξι διαστάσεων που έχει μια (διατεταγμένη) βάση που δίνεται από τις γραμμές του πίνακα M ,

$$M = \begin{pmatrix} 19 & 2 & 32 & 46 & 3 & 33 \\ 15 & 42 & 11 & 0 & 3 & 24 \\ 43 & 15 & 0 & 24 & 4 & 16 \\ 20 & 44 & 44 & 0 & 18 & 15 \\ 0 & 48 & 35 & 16 & 31 & 31 \\ 48 & 33 & 32 & 9 & 1 & 29 \end{pmatrix}$$

Παρατηρούμε ότι $||v_1||=67.845$,
$||v_2||=51.913$,
$||v_3||=54.055$,
$||v_4||=69.433$,
$||v_5||=75.544$,
$||v_6||=73.075$.
Επομένως το μικρότερο διάνυσμα είναι το v_2. Ακόμα έχουμε det(M)=777406251. Υπολογίζουμε το λόγο Hadamard.
Έχουμε H(M) $=\left(\frac{\det(M)}{\|v_1\|\|v_2\|\|v_3\|\|v_4\|\|v_5\|\|v_6\|}\right)^{1/6}= 0.4691$. Δηλαδή τα διανύσματα της βάσης απέχουν πολύ από το να είναι ορθογώνια.
Εφαρμόζοντας τώρα τον αλγόριθμο LLL στον M παίρνουμε τη βάση που αποτελείται από τις γραμμές του πίνακα M^{LLL} δηλαδή

$$M^{LLL} = \begin{pmatrix} 7 & -12 & -8 & 4 & 19 & 9 \\ -20 & 4 & -9 & 16 & 13 & 16 \\ 5 & 2 & 33 & 0 & 15 & -9 \\ -6 & -7 & -20 & -21 & 8 & -12 \\ -10 & -24 & 21 & -15 & -6 & -11 \\ 7 & 4 & -9 & -11 & 1 & 31 \end{pmatrix}$$

Έχουμε $||v_1^{LLL}||$=26.739,
$||v_2^{LLL}||$=34.322,
$||v_3^{LLL}||$=37.735,
$||v_4^{LLL}||$=33.674,
$||v_5^{LLL}||$=38.716,
$||v_6^{LLL}||$=35.071.

Επομένως το μικρότερο διάνυσμα είναι το v_1^{LLL} , σημαντικά μικρότερο του v_2. Παρατηρούμε ότι σ(L)=(3!detL)$^{1/3}$/√ π = 23.062. Δηλαδή το αναμενόμενο μικρότερο διάνυσμα είναι πολύ κοντά σε αυτό που βρήκαμε με τον αλγόριθμο LLL. Ακόμα det(M^{LLL})=-777306251 δηλαδή |det(M)|=|det(M^{LLL})|. Τέλος, υπολογίζουμε το λόγο Hadamard του M^{LLL} και βρίσκουμε H(M^{LLL})=0.882, που σημαίνει ότι τα διανύσματα της βάσης που βρήκαμε είναι πολύ κοντά στο να είναι ορθογώνια από τα αρχικά.

Αν αντιστρέψουμε τη σειρά των γραμμών του M και εφαρμόσουμε τον αλγόριθμο LLL παίρνουμε

$$M^{LLL} = \begin{pmatrix} -7 & 12 & 8 & -4 & -19 & -9 \\ 20 & -4 & 9 & -16 & -13 & -16 \\ 5 & 2 & 33 & 0 & 15 & -9 \\ -6 & -7 & -20 & -21 & 8 & -12 \\ -10 & -24 & 21 & -15 & -6 & -11 \\ 7 & 4 & -9 & -11 & 1 & 31 \end{pmatrix}$$

Παρατηρούμε ότι το μικρότερο διάνυσμα είναι πάλι το v_2 όμως τώρα H(M^{LLL}) =0.879 δηλαδή λίγο μικρότερο από το προηγούμενο. Αυτό μας δείχνει ότι η σειρά των διανυσμάτων της βάσης επηρεάζει τον αλγόριθμο.

4.3) Γενικεύσεις του αλγόριθμου LLL

Ο αλγόριθμος LLL χρησιμοποιείται αρκετό διάστημα ώστε να έχουν βρεθεί βελτιώσεις και γενικεύσεις. Συνήθως σε αυτές θυσιάζεται η ταχύτητα του αλγορίθμου προκειμένου να πάρουμε καλύτερα αποτελέσματα.

Μία βελτίωση αφορά το βήμα ανταλλαγής (βήμα (11) του αλγόριθμου LLL). Κανονικά, ανταλλάσσουμε το v_k με το v_{k-1}. Αντί για αυτό, εισάγουμε το v_k μεταξύ των v_i και v_{i-1}, όπου το i είναι τέτοιο ώστε να επιτυγχάνεται μεγάλη αναγωγή μεγέθους (βήμα (6)). Η μέθοδος αυτή λέγεται μέθοδος της βαθειάς εισαγωγής (deep insertion method). Στη χειρότερη περίπτωση ο αλγόριθμος δεν είναι πολυωνυμικού χρόνου αλλά στην πράξη στις περισσότερες περιπτώσεις είναι πιο γρήγορος και επιστρέφει καλύτερες βάσεις από τον LLL.

Μία άλλη βελτίωση που μπορούμε να κάνουμε έχει να κάνει με τον ορισμό της ανηγμένης βάσης. Αντί για την LLL ανηγμένη βάση θεωρούμε μία άλλη με ιδιότητες τέτοιες που θα μας εξασφαλίζουν ότι η βάση που θα επιστρέφει ο αλγόριθμος θα είναι καλύτερη από του LLL.

Έστω λοιπόν τα διανύσματα $v_1,v_2,\ldots$ και για $i\geq 1$ έστω $v_1^*,v_2^*,\ldots$ τα αντίστοιχα διανύσματα που παίρνουμε από τη μέθοδο Gram-Schmidt. Θεωρούμε την απεικόνιση $\pi:L\rightarrow R^n$, $\pi_i(v)=v-\sum_{j=1}^{i}\frac{v\cdot v_j^*}{\left\|v_j^*\right\|^2}v_j^*$. Επίσης έχουμε $\pi_0(v)=v$.

Ορισμός 4.9) Έστω L ένα πλέγμα. Μία βάση $v_1,v_2,\ldots,v_n$ λέγεται Korkin-Zolotarev (KZ) ανηγμένη αν ικανοποιεί τις ακόλουθες τρεις προυποθέσεις :

Α) Το v_1 είναι το μικρότερο μη μηδενικό διάνυσμα στο L.

Β) Για $i=1,2,3,\ldots,n$ διαλέγουμε το διάνυσμα v_i τέτοιο ώστε το $\pi_{i-1}(v_i)$ να είναι το μικρότερο μη μηδενικό διάνυσμα στο $\pi_{i-1}(L)$.

Γ) Για όλα τα i,j με $1\leq i<j\leq n$ έχουμε $|\pi_{i-1}(v_i)\cdot\pi_{i-1}(v_j)|\leq\|\pi_{i-1}(v_i)\|^2$.

Μία KZ ανηγμένη βάση είναι καλύτερη από μία LLL βάση γιατί εξ'ορισμού το πρώτο της διάνυσμα είναι το μικρότερο του πλέγματος (και μία λύση για το SVP). Το τίμημα όμως είναι ότι οι αλγόριθμοι για την εύρεση μιας τέτοιας βάσης είναι εκθετικού χρόνου. Ο πιο γνωστός είναι ο BKZ-LLL(όπου BKZ σημαίνει Block Korkin-Zolotarev) και είναι μία παραλλαγή του LLL, όπου το βήμα της αναγωγής

γίνεται ανά μπλοκ. Έτσι, ενώ στον LLL γίνεται μεταξύ των v_k και v_{k-1}, εδώ γίνεται σε ένα μπλοκ διανυσμάτων μήκους β, δηλαδή $v_k,v_{k+1},\ldots,v_{k+\beta-1}$ και παίρνουμε μία KZ ανηγμένη βάση για το υποπλέγμα που παράγεται από το μπλοκ των διανυσμάτων. Όσο μεγαλύτερο είναι το β τόσο περισσότερο χρόνο χρειάζεται ο αλγόριθμος αλλά και τόσο καλύτερο είναι το τελικό αποτέλεσμα. Πράγματι αποδεικνύεται ότι ο BKZ-LLL έχει παράγοντα προσέγγισης για το SVP $\beta^{n/\beta}$ όταν το LLL έχει $2^{n/2}$,(καλύτερο),ενώ χρειάζεται $O(\beta^{c\beta}n^d)$ βήματα με c,d μικρές σταθερές, (δηλαδή παίρνοντας $\beta\approx n/\delta$ όπου n η διάσταση του πλέγματος και δ μία σταθερά βλέπουμε ότι απαιτείται εκθετικός ως προς n χρόνος για να τερματίσει ο αλγόριθμος).

Κεφάλαιο 5) Κρυπτοσυστήματα και εφαρμογές του αλγορίθμου LLL

5.1) Εισαγωγή

Στο κεφάλαιο αυτό θα περιγράψουμε τρία κρυπτοσυστήματα και πως με τη χρήση του αλγορίθμου LLL μπορούμε να τα κρυπταναλύσουμε. Τα κρυπτοσυστήματα αυτά είναι το Merkle-Hellman, το GGH και το NTRU. Και τα τρία είτε βασίζονται σε πλέγματα είτε μπορούν να διατυπωθούν με χρήση πλεγμάτων. Ας σημειωθεί εδώ ότι αυτά είναι μόνο τρία παραδείγματα χρήσης του LLL στην κρυπτογραφία και σε καμία περίπτωση δεν εξαντλούν τις εφαρμογές του. Χαρακτηριστικό παράδειγμα είναι η χρήση του LLL για το "σπάσιμο" του RSA όταν $N=p^rq$ για μικρό r. Από τα τρία κρυπτοσυστήματα που επιλέξαμε το πρώτο χαρακτηρίζεται από απλότητα και είναι έτσι εύκολο να δούμε τον τρόπο με τον οποίο γίνεται η εφαρμογή του αλγορίθμου. Το δεύτερο βασίζεται κατευθείαν στο CVP και στον αλγόριθμο του Babai που αναφέραμε. Είχε γίνει πολύ γνωστό όταν πρωτοεμφανίστηκε γιατί οι δημιουργοί του έδωσαν μια σειρά από προβλήματα-προκλήσεις, υποστηρίζοντας ότι για n>300 το κρυπτοσύστημα θα ήταν αδύνατο να κρυπταναλυθεί. Όμως ο Nguyen με χρήση του LLL και ενός έξυπνου μετασχηματισμού ώστε από το αρχικό CVP να καταλήξει σε ένα πιο εύκολο, έλυσε αυτά τα προβλήματα για n μέχρι 350 (CRYPTO 99). Για μεγαλύτερο n το κρυπτοσύστημα δεν είναι πρακτικό. Το τρίτο είναι το πιο πετυχημένο από πρακτικής πλευράς. Βασίζεται, από μαθηματικής πλευράς σε πολυωνυμικούς δακτυλίους πηλίκο, όμως το πρόβλημα στο οποίο στηρίζεται μπορεί εύκολα να διατυπωθεί ως SVP (ανάκτηση κλειδιού) ή CVP (ανάκτηση αρχικού κειμένου) για μία ειδική κατηγορία πλεγμάτων.

Δυστυχώς αν και τα κρυπτοσυστήματα που βασίζονται σε πλέγματα είναι πιο γρήγορα από τα υπόλοιπα η έρευνα για την ασφάλεια τους δεν έχει προχωρήσει πολύ σε σύγκριση με αυτά που βασίζονται στην παραγοντοποίηση ή στο πρόβλημα του διακριτού λογάριθμου. Συνεπώς, παρά την θεωρητική μελέτη και έρευνα, οι πρακτικές υλοποιήσεις είναι ελάχιστες και από αυτές οι περισσότερες αφορούν το NTRU.

Κατά την παρουσίαση των κρυπτοσυστημάτων ακολουθώντας την παράδοση ονομάζουμε Bob τον αποστολέα του μηνύματος, Alice τον παραλήπτη και Eve αυτήν που υποκλέπτει το κρυπτογραφημένο μήνυμα και θέλει να το "σπάσει".

5.2)Το κρυπτοσύστημα Merkle-Hellman

Το κρυπτοσύστημα Merkle-Hellman είναι η πρώτη προσπάθεια για τη δημιουργία ενός κρυπτοσυστήματος που να βασίζεται σε ένα NP-πλήρες πρόβλημα. Το πρόβλημα στο οποίο στηρίζεται είναι το πρόβλημα αθροίσματος υποσυνόλου (subset sum problem) που αποτελεί γενίκευση του προβλήματος του σακιδίου (knapsack problem).

Ορισμός 5.1) Το πρόβλημα του αθροίσματος υποσυνόλου (subset sum)

Έστω ένα σύνολο θετικών ακεραίων $M=(M_1,M_2,\ldots,M_n)$ και ένας ακέραιος S. Να βρεθεί ένα υποσύνολο του M που το άθροισμα των στοιχείων του να είναι ίσο με S.

Ένας άλλος τρόπος να περιγράψουμε το πρόβλημα αυτό είναι ως εξής: Έστω ένα σύνολο θετικών ακεραίων $M=(M_1,M_2,\ldots,M_n)$ και ένας ακέραιος S. Να βρεθεί το

δυαδικό διάνυσμα $x=(x_1,x_2,\ldots,x_n)$ (δηλαδή κάθε x_i είναι μηδέν ή ένα) ώστε $S = \sum_{i=1}^{n} x_i M_i$.

Όπως έχουμε αναφέρει το πρόβλημα αυτό είναι NP-πλήρες και επομένως είναι δύσκολο να επιλυθεί υπολογιστικά. Υπάρχει όμως μία ειδική περίπτωση του προβλήματος η οποία είναι πολύ εύκολο να λυθεί. Δίνουμε καταρχήν τον ακόλουθο ορισμό:

Ορισμός 5.2)Υπεραυξητική ακολουθία

Μία ακολουθία $r=(r_1,r_2,\ldots,r_n)$ θετικών ακεραίων λέγεται υπεραυξητική αν ισχύει $r_{i+1}\geq 2r_i$ για $1\leq i\leq n-1$.

Ισχύει το ακόλουθο λήμμα που δείχνει γιατί έχουν ονομαστεί έτσι.

Λήμμα 5.3) Έστω $r=(r_1,r_2,\ldots,r_n)$ μία υπεραυξητική ακολουθία. Τότε

$r_k>r_{k-1}+r_{k-2}+\ldots+r_2+r_1$ για $2\leq k\leq n$.

Απόδειξη

Με επαγωγή. Πράγματι, για k=2 έχουμε $r_2\geq 2r_1\geq r_1$. Έστω ότι το λήμμα ισχύει για k=i. Τότε για k=i+1 έχουμε $r_{i+1}\geq 2r_i=r_i+r_i>r_i+(r_{i-1}+r_{i-2}+\ldots+r_2+r_1)$ δηλαδή ισχύει για i+1 άρα εξ'επαγωγής ισχύει για $2\leq k\leq n$.

Όταν το σύνολο M στο πρόβλημα αθροίσματος υποσυνόλου είναι υπεραυξητική ακολουθία λύνεται πολύ εύκολα με τον ακόλουθο τρόπο:

1)Επανέλαβε για i=n μέχρι 1

2)Αν $S\geq M_i$ θέσε $x_i=1$ και αφαίρεσε το M_i από το S

3)Αλλιώς θέσε $x_i=0$

4)Τέλος βρόχου

Παράδειγμα) Έστω M=(4,9,20,41,87) μια υπεραυξητική ακολουθία και S=111.Τότε εφαρμόζοντας τον παραπάνω αλγόριθμο έχουμε $S\geq 87$ άρα $x_5=1$ και S=111-87=24. Τώρα $S\leq 41$ άρα $x_4=0$.Συνεχίζοντας έτσι έχουμε $S\geq 20$ άρα $x_3=1$ και S=24-20=4, $S\leq 9$ άρα $x_2=0$,S=4 άρα $x_1=1$. Συνεπώς, παίρνουμε x=(1,0,1,0,1).

Στο κρυπτοσύστημα των Merkle-Hellman, και όσα το ακολούθησαν και βασίζονται σε αυτό, η υπεραυξητική ακολουθία παίζει το ρόλο της συνάρτησης καταπακτής (trapdoor function). Έτσι μία υπεραυξητική ακολουθία παίζει το ρόλο του ιδιωτικού κλειδιού και με κάποιο (μυστικό) τρόπο (για παράδειγμα με πολλαπλασιασμό και μετά μείωση μέσω ισοτιμίας με κάποιο modulo ,ή και διαδοχική εφαρμογή αυτής της διαδικασίας) μετατρέπεται σε μία απλή ακολουθία που αποτελεί το δημόσιο κλειδί και για την οποία η Eve χρειάζεται να λύσει το subset-sum στη γενική του μορφή. Όλες οι τροποποιήσεις και βελτιώσεις του, δεν μπόρεσαν να το κάνουν ασφαλές εκτός όταν πάμε σε μεγάλες διαστάσεις που δεν είναι πρακτικό λόγω του μεγάλου μεγέθους κλειδιού που απαιτείται, παρόλο που είναι πολύ πιο γρήγορο από τα άλλα κρυπτοσυστήματα δημοσίου κλειδιού γιατί χρειάζεται μόνο λίγους πολλαπλασιασμούς με ισοτιμία.

Ξεκινάμε την περιγραφή του κρυπτοσυστήματος από τον τρόπο δημιουργίας κλειδιών. Η Alice λοιπόν, που θέλει να λάβει μήνυμα από τον Bob, επιλέγει μια υπεραυξητική ακολουθία $r=(r_1,r_2,\ldots,r_n)$ και δύο μεγάλους ακεραίους Α και Β τέτοιους ώστε $B>2r_n$ και ΜΚΔ(A,B)=1. Αυτά αποτελούν το ιδιωτικό κλειδί της Alice. Η Alice κατασκευάζει μια νέα μη υπεραυξητική ακολουθία Μ θέτοντας $M_i=Ar_i \pmod B$ με $0\leq M_i<B$. Αυτή είναι το δημόσιο κλειδί της Alice.

Ο Bob που θέλει να στείλει ένα μήνυμα στην Alice το μετατρέπει σε ένα δυαδικό διάνυσμα x και υπολογίζει το $S=xM=\sum_{i=1}^{n} x_i M_i$ που αποτελεί το κρυπτογραφημένο μήνυμα .

Η Alice για να αποκρυπτογραφήσει το μήνυμα του Bob υπολογίζει καταρχήν το $S'=A^{-1}S \pmod B$ με $0\leq S'<B$. Στη συνέχεια λύνει εύκολα το πρόβλημα του αθροίσματος υποσυνόλου για το S' με την υπεραυξητική ακολουθία r. Παρατηρούμε ότι $S'= A^{-1}S \pmod B= A^{-1} \sum_{i=1}^{n} x_i M_i \pmod B=$

$=A^{-1} \sum_{i=1}^{n} x_i Ar_i \pmod B= \sum_{i=1}^{n} x_i r_i \pmod B$. Επειδή $B>2r_n$ και η r είναι υπεραυξητική ακολουθία έχουμε $\sum_{i=1}^{n} x_i r_i \leq \sum_{i=1}^{n} r_i<2r_n<B$ και επειδή $0<S'<B$ η Alice παίρνει την ισότητα $S'= \sum_{i=1}^{n} x_i r_i$ και όχι ισοτιμία.

Σχηματικά το κρυπτοσύστημα Merkle-Hellman έχει ως εξής:

Merkle-Hellman	
Alice	Bob
Δημιουργία Κλειδιού	
Διάλεξε υπεραυξητική ακολουθία $r=(r_1,r_2,...,r_n)$,A,B ακέραιους με $B>2r_n$ και ΜΚΔ(A,B)=1. Υπολόγισε τα $M_i=Ar_i \pmod B$,$1\leq i\leq n$. Δημόσιο κλειδί $M=(M_1,M_2,\ldots,M_n)$	
Κρυπτογράφηση	
	Έστω x το μήνυμα (δυαδικό διάνυσμα) S=xM το κρυπτογραφημένο μήνυμα
Αποκρυπτογράφηση	
Υπολόγισε $S'=A^{-1}S \pmod B$ Λύσε το πρόβλημα αθροίσματος υποσυνόλου με S' και r.Το μήνυμα x ικανοποιεί την xr=S'	

Πριν δούμε πως το μπορούμε να εκφράσουμε το κρυπτοσύστημα με τη βοήθεια πλεγμάτων ας δούμε τι τιμές παίρνουν οι παράμετροί του. Υποθέτοντας ότι έχουμε διαλέξει το n πρέπει $r_1>2^n$ γιατί αλλιώς έχουν βρεθεί εύκολες επιθέσεις .Όμως τότε $r_n>2r_{n-1}>4r_{n-2}>\ldots>2^n r_1>2^{2n}$.Άρα $B>2r_n=2^{2n+1}$ και επομένως $M_i=O(2^{2n})$ και $S=O(2^{2n})$.Δηλαδή για ένα μήνυμα n bits το κρυπτοκείμενο είναι 2n bits και το δημόσιο κλειδί μια λίστα n ακεραίων με το καθένα 2n bits.

Θεωρούμε τώρα τον (n+1)x(n+1) πίνακα $A_{M,S}=\begin{pmatrix} 2 & 0 & 0 & \dots & 0 & m_1 \\ 0 & 2 & 0 & \dots & 0 & m_2 \\ 0 & 0 & 2 & \dots & 0 & m_3 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & 0 & \cdots & 2 & m_n \\ 1 & 1 & 1 & \cdots & 1 & S \end{pmatrix}$
όπου η τελευταία στήλη περιέχει το δημόσιο κλειδί και το κρυπτοκείμενο και τα διανύσματα γραμμές
$v_1=(2,0,\dots,m_1),\dots,v_2=(0,2,\dots,0,m_2),v_n=(0,\dots,2,m_n),v_{n+1}=(1,1,\dots,1,S)$ αποτελούν μια βάση του (n+1)x(n+1) πλέγματος L. Έστω x μία λύση του subset-sum, τότε το L περιέχει το διάνυσμα $t=\sum_{i=1}^{n} x_i v_i - v_{n+1}=(2x_1-1,2x_2-1,\dots,2x_n-1,0)$ όπου η τελευταία συντεταγμένη είναι μηδέν γιατί $S=\sum_{i=1}^{n} x_i M_i$.Αφού όμως τα x_i είναι μηδέν ή ένα, τα $2x_i-1$ είναι ένα ή μείον ένα και επομένως $\|t\| = \sqrt{n}$.Όμως, όπως είδαμε $m_i=O(2^n)$ και $S=O(2^n)$ και συνεπώς $\|v_i\|=O(2^n)$.Δηλαδή είναι πολύ δύσκολο το L να περιέχει άλλα μη μηδενικά διανύσματα τόσο μικρά όσο το t.Συνεπώς με τον αλγόριθμο LLL βρίσκοντας το μικρότερο διάνυσμα του πλέγματος L βρίσκουμε το t που είναι λύση του subset-sum και άρα σπάμε το κρυπτοσύστημα.

Δίνουμε τώρα ένα παράδειγμα:

Παράδειγμα Merkle Hellman

Έστω r=(3,11,24,50,115),A=113,B=250 το ιδιωτικό κλειδί της Alice.Τότε το δημόσιο κλειδί M είναι M=(113*3,113*11,113*24,113*50,113*115)(mod 250)=(89,243,212,150,245), μία προφανώς μη υπεραυξητική ακολουθία.
Έστω τώρα ότι ο Bob θέλει να στείλει το μήνυμα x=(1,0,1,0,1). Το κρυπτογραφεί ως S=xM=1*89+0*243+1*212+0*150+1*245=546.
Η Alice βρίσκει καταρχήν τον αντίστροφο του 113 modulo 250 που είναι το 177 και το πολλαπλασιάζει με το μήνυμα που έλαβε από τον Bob δηλαδή S'=177*546 (mod 250) =142 (mod 250).Εφαρμόζοντας τον αλγόριθμο παίρνει 142=1*115+0*50+1*24+0*11+1*3 δηλαδή x=(1,0,1,0,1) που είναι το μήνυμα του Bob.
Ας δούμε τώρα πως η Eve μπορεί να σπάσει το μήνυμα του Bob. Καταρχήν σχηματίζει τον πίνακα $A_{M,S}=\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 89 \\ 0 & 2 & 0 & 0 & 0 & 243 \\ 0 & 0 & 2 & 0 & 0 & 212 \\ 0 & 0 & 0 & 2 & 0 & 150 \\ 0 & 0 & 0 & 0 & 2 & 245 \\ 1 & 1 & 1 & 1 & 1 & 546 \end{pmatrix}$,
εφαρμόζει τον LLL για το πλέγμα με βάση τις γραμμές του πίνακα και παίρνει τον $\begin{pmatrix} -1 & 1 & -1 & 1 & -1 & 0 \\ 1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & 1 & 2 \\ 1 & -1 & -1 & -1 & -1 & 2 \\ -2 & -2 & 4 & 0 & -2 & 0 \\ -6 & -4 & -6 & -6 & 0 & -3 \end{pmatrix}$.
Το μικρότερο διάνυσμα είναι το (-1,1,-1,1,-1,0) το οποίο εκφράζουμε ως γραμμικό συνδυασμό της αρχικής βάσης δηλαδή (-1,1,-1,1,-1,0)=(-1,0,-1,0,-1,1)$A_{M,S}$. Το διάνυσμα (-1,0,-1,0,-1,1) μας δίνει τη λύση .Πράγματι -89-212-245+546=0 άρα x=(1,0,1,0,1).

5.3) Το κρυπτοσύστημα GGH

Η Alice ξεκινά διαλέγοντας n γραμμικά ανεξάρτητα διανύσματα $v_1,v_2,\ldots,v_n \in Z^n$,σαν βάση, τα οποία είναι κοντά στο να είναι ορθογώνια μεταξύ τους, δηλαδή ο λόγος Hadamard της βάσης να είναι κοντά στο 1. Αυτά αποτελούν το ιδιωτικό της κλειδί. Ονομάζουμε V τον nxn πίνακα που οι γραμμές του είναι τα διανύσματα $v_1,v_2,\ldots,v_n$, και L το πλέγμα που δημιουργείται από αυτά τα διανύσματα.

Η Alice συνεχίζει διαλέγοντας έναν nxn ακέραιο πίνακα U με |det(U)|=1, και υπολογίζει τον W=UV. Τα διανύσματα που παίρνουμε από τις γραμμές του $W,w_1,w_2,\ldots,w_n$, είναι όπως ξέρουμε μία νέα βάση για το L και αποτελούν το δημόσιο κλειδί της Alice.

Επομένως ο Bob,που θέλει να στείλει ένα μήνυμα στην Alice, γνωρίζει το δημόσιο κλειδί της. Έστω m ένα μικρό (σε σχέση με τα v_i,w_i) διάνυσμα που αποτελεί το μήνυμα του Bob (με κάποια κατάλληλη κωδικοποίηση) και r ένα επίσης μικρό τυχαίο διάνυσμα διαταραχής που διαλέγει ο Bob που χρησιμεύει ως προσωρινό κλειδί. Συνήθως το r υπολογίζεται εφαρμόζοντας μια συνάρτηση κατακερματισμού (hash function) στο μήνυμα m.Ο Bob υπολογίζει το $e=mW+r=\sum_{i=1}^{n} m_i w_i + r$ που αποτελεί το κρυπτογραφημένο κείμενο. Προφανώς το e δεν ανήκει στο πλέγμα L αλλά είναι κοντά στο σημείο mW αφού το r είναι μικρό.

Για να αποκρυπτογραφήσει τώρα η Alice το μήνυμα του Bob αρκεί να εφαρμόσει τον αλγόριθμο του Babai με την καλή βάση που είναι το ιδιωτικό της κλειδί. Αφού το r είναι μικρό το σημείο που βρίσκει είναι το mW, οπότε πολλαπλασιάζοντας με W^{-1} βρίσκει το m. Αντίθετα η Eve που έχει την βάση από το δημόσιο κλειδί, αν δοκιμάσει να εφαρμόσει τον αλγόριθμο του Babai θα αποτύχει γιατί όπως έχουμε πει ο αλγόριθμος επιτυγχάνει όταν τα διανύσματα της βάσης είναι σχεδόν ορθογώνια μεταξύ τους. Εφαρμόζοντας όμως τον αλγόριθμο LLL μπορεί να βρει μια καλή βάση και τελικά να αποκρυπτογραφήσει το μήνυμα.

Σχηματικά το σύστημα GGH έχει ως εξής:

GGH	
Alice	Bob
Δημιουργία Κλειδιού	
Βρες καλή βάση $v_1,v_2,\ldots,v_n$ Βρες ακέραιο U nxn με |det(U)|=1 Βρες κακή βάση $w_1,w_2,\ldots,w_n$ από τις γραμμές του W=UV. Δημόσιο κλειδί = $w_1,w_2,\ldots,w_n$	
Κρυπτογράφηση	
	Έστω m το μήνυμα Διάλεξε τυχαίο μικρό διάνυσμα r e=mW+r το κρυπτογραφημένο μήνυμα
Αποκρυπτογράφηση	
Με τον αλγόριθμο του Babai υπολόγισε το $v \in L$ που είναι πλησιέστερο του e. Υπολόγισε το αρχικό μήνυμα $m=vW^{-1}$	

Παράδειγμα GGH

Έστω v_1=(-97,19,19), v_2=(-36,30,86), v_3=(-184,-64,78), το ιδιωτικό κλειδί (η καλή βάση) της Alice. Είναι det(L)=859516 και
H(v_1,v_2,v_3)=$(\frac{\det(L)}{\|v_1\|\|v_2\|\|v_3\|})^{1/3}$≈0.74620.Έστω ακόμα
U=$\begin{pmatrix} 4327 & -15447 & 23454 \\ 3297 & -11770 & 17871 \\ 5464 & -19506 & 29617 \end{pmatrix}$ με det(U)=-1. Επομένως το δημόσιο κλειδί της Alice είναι w_1=(-4179163,-1882253,583183),w_2=(-3184353,-1434201,444361),w_3=(-5277320,-2376852,736426) και H(w_1,w_2,w_3)≈0.0000208.
Έστω τώρα ότι το μήνυμα που θέλει να στείλει ο Bob είναι m=(86,-35,-32) και το τυχαίο διάνυσμα διαταραχής r=(-4,-3,2). Επομένως το κρυπτογραφημένο μήνυμα που θα στείλει ο Bob στην Alice είναι e=mW+r δηλαδή e=(-79081427,-35617462,11035473).
Για την αποκρυπτογράφηση η Alice εφαρμόζει τον αλγόριθμο του Babai, δηλαδή γράφει το e σαν γραμμικό συνδυασμό της καλής βάσης (του ιδιωτικού της κλειδιού) με πραγματικούς συντελεστές δηλαδή e≈81878.97v_1-292300v_2+443815.04v_3. Στρογγυλοποιώντας τους συντελεστές στον πλησιέστερο ακέραιο παίρνουμε το διάνυσμα v∈ L, v=(-79081423,-35617459,11035471) που είναι κοντά στο e. Τέλος ανακτά το m γράφοντας το v σαν γραμμικό συνδυασμό της δημόσιας βάσης και κρατώντας τους συντελεστές. Πράγματι έχουμε v=86w_1-35w_2-32w_3 και m=(86,-35,-32) που είναι το μήνυμα του Bob. Ας παρατηρήσουμε ότι αν η Eve χρησιμοποιούσε τον αλγόριθμο του Babai με την δημόσια βάση θα έπαιρνε e≈75.76w_1-34.52w_2-24.18w_3, οπότε στρογγυλοποιώντας παίρνει το v'∈ L , v'=76w_1-35w_2-24w_3=(-79508353,-35809745,11095049) που δίνει το λάθος μήνυμα m'=(76,-35,-24). Ακόμα έχουμε ||e-v||≈5.3852 ενώ ||e-v'||≈472000 που δείχνει την αποτυχία του αλγορίθμου του Babai στην δεύτερη περίπτωση.

Η Eve όμως έχει και μια δεύτερη επιλογή, να εφαρμόσει τον αλγόριθμο LLL στο δημόσιο κλειδί . Με αυτόν τον τρόπο βρίσκει την βάση $\begin{pmatrix} 36 & -30 & -86 \\ 61 & 11 & 67 \\ -10 & 102 & -40 \end{pmatrix}$ με H=0.956083 (καλύτερο από της ιδιωτικής βάσης). Στη συνέχεια η Eve εφαρμόζει τον αλγόριθμο του Babai και βρίσκει το διάνυσμα v=(79081423,35617459,-11035471)=-86w_1+35w_2+32w_3 και ανακτά το αρχικό μήνυμα (-86,35,32).

Όπως φαίνεται και από το παράδειγμα, με τον αλγόριθμο LLL το GGH δεν είναι ασφαλές, εκτός αν χρησιμοποιήσουμε πλέγμα μεγάλης διάστασης (n>400) αλλά τότε δεν είναι πρακτικό. (το δημόσιο κλειδί έχει μέγεθος της τάξης των 128Kbytes).

5.4) Το κρυπτοσύστημα NTRU

Το κρυπτοσύστημα NTRU, στην αρχική περιγραφή του βασίζεται σε πολυωνυμικούς δακτυλίους modulo m, αλλά μπορεί να περιγραφεί και με την χρήση πλεγμάτων. Ξεκινάμε λοιπόν την παρουσίαση του με βάση τους δακτυλίους και μετά θα αναφερθούμε και στην σχέση του με τα πλέγματα.
Διαλέγουμε καταρχήν ακεραίους N≥1 ,p,q,d, με N,p πρώτους, ΜΚΔ(N,q)=ΜΚΔ(p,q)=1και q>(6d-1)p και θεωρούμε τους δακτυλίους

$$R = \frac{Z[x]}{(x^N - 1)}, \qquad R_p = \frac{(Z/pZ)[x]}{(x^N - 1)}, \quad R_q = \frac{(Z/qZ)[x]}{(x^N - 1)}$$

Δίνουμε τους ακόλουθους ορισμούς:

Ορισμός 5.4) Έστω a(x) ∈ R_q, ένα πολυώνυμο . Το centered lift του a(x) στο R είναι το μοναδικό πολυώνυμο a'(x) που ικανοποιεί a'(x) mod q= a(x) , που οι συντελεστές του ικανοποιούν τη σχέση $\frac{-q}{2} \leq a_i' \leq \frac{q}{2}$.
Έτσι έχουμε τον τρόπο να μεταφέρουμε ένα πολυώνυμο από το R_q στο R.
Ορισμός 5.4.2)Για d_1,d_2 θετικούς ακεραίους συμβολίζουμε με
$T(d_1,d_2)$={a(x) ∈ R : a(x) έχει d_1 συντελεστές ίσους με 1
a(x) έχει d_2 συντελεστές ίσους με -1
a(x) έχει τους υπόλοιπους συντελεστές ίσους με 0 }
Τα πολυώνυμα που ανήκουν στο $T(d_1,d_2)$ λέγονται τριαδικά (ternary ή trinary) πολυώνυμα.

Η Alice διαλέγει δύο πολυώνυμα f(x) ∈ T(d+1,d) και g(x) ∈ T(d,d), και υπολογίζει τους αντίστροφους του f(x), $F_q(x)=f(x)^{-1}$∈R_q και $F_p(x)=f(x)^{-1}$ ∈ R_p. Αν οι αντίστροφοι δεν υπάρχουν τότε επιλέγει καινούρια f(x). Στη συνέχεια υπολογίζει το $h(x)=F_q(x)*g(x)$ ∈ R_q. Τα f,g είναι το ιδιωτικό της κλειδί και το h το δημόσιο.
Ο Bob κωδικοποιεί το μήνυμα του ως ένα πολυώνυμο m(x) ∈ R που οι συντελεστές του είναι μεταξύ $\frac{-1}{2}p$ και $\frac{1}{2}$p. Ακόμα διαλέγει ένα τυχαίο πολυώνυμο r(x) ∈T(d,d) και υπολογίζει το $e(x) \equiv ph(x) * r(x) + m(x)\ (mod\ q)$. Αυτό είναι το κρυπτοκείμενο του Bob και προφανώς ανήκει στο δακτύλιο R_q.
Η Alice για να αποκρυπτογραφήσει το κρυπτοκείμενο του Bob υπολογίζει το $a(x) \equiv f(x) * e(x)\ \ (mod\ q)$ και στη συνέχεια μετατρέπει (με centered lift) το a(x) από στοιχείο του R_q σε στοιχείο του R. Τέλος, υπολογίζει το
$b(x) \equiv F_p(x) * a(x)(mod\ p)$. Εφόσον έχει γίνει σωστή επιλογή των αρχικών παραμέτρων το b(x) ταυτίζεται με το αρχικό μήνυμα m(x).Το επεξηγούμε καλύτερα με την παρακάτω πρόταση.

Πρόταση 5.5) Αν οι παράμετροι του NTRU (N,p,q,d) είναι τέτοιες ώστε q>(6d+1)p, τότε το b(x) ταυτίζεται με το m(x).

Απόδειξη

Πράγματι, έχουμε: $a(x) \equiv f(x) * e(x)(mod\ q)$
$\equiv f(x) * \big(ph(x) * r(x) + m(x)\big)(mod\ q)$
$\equiv pf(x) * F_q(x) * g(x) * r(x) + f(x) * m(x)(mod\ q)$
$\equiv pg(x) * r(x) + f(x) * m(x)(mod\ q)$

Θεωρούμε τώρα το πολυώνυμο $pg(x) * r(x) + f(x) * m(x)$ στο R και όχι στο R_q (το οποίο μπορούμε εύκολα να πετύχουμε με ένα centered lift). Εφόσον τα g(x) και r(x) ανήκουν στο T(d,d) ο μεγαλύτερος συντελεστής του γινομένου g(x)*r(x) είναι 2d.Όμοια, το f(x) ανήκει στο T(d+1,d) ενώ οι συντελεστές του m είναι μεταξύ $\frac{-1}{2}p$ και $\frac{1}{2}$p, άρα οι συντελεστές του γινομένου τους είναι μεταξύ (2d+1) $\frac{1}{2}$p.Επομένως ο μεγαλύτερος συντελεστής που μπορεί να προκύψει είναι το πολύ 2dp+(2d+1) $\frac{1}{2}$p=(3d+$\frac{1}{2}$)p δηλαδή μικρότερος από $\frac{1}{2}$q. Επομένως το $pg(x) * r(x) + f(x) * m(x)$ είτε υπολογιστεί στο R_q είτε στο R είναι το ίδιο, δηλαδή
a(x)= $pg(x) * r(x) + f(x) * m(x)$, στο R.

Συνεπώς, b(x)= $F_p(x)*a(x)$
$= F_p(x)*(pg(x)*r(x)+f(x)*m(x))$ και παίρνοντας modulo p
$\equiv F_p(x) * f(x) * m(x)(mod\ p)$
$\equiv m(x)(mod\ p)$.

Σχηματικά το σύστημα NTRU έχει ως εξής:

NTRU	
Επιλογή παραμέτρων	
Παράμετροι (N,p,q,d) με N,p πρώτους,ΜΚΔ(p,q)=ΜΚΔ(N,q)=1 και q>(6d+1)p	
Alice	Bob
Δημιουργία Κλειδιού	
Διάλεξε ιδιωτικό f ∈ T(d+1,d) αντιστρέψιμο στα R_p,R_q. Διάλεξε ιδιωτικό g∈T(d,d).Υπολόγισε F_p,F_q, τα αντίστροφα του f στα Rp,R_q αντίστοιχα. Δημόσιο κλειδί $h=F_q*g$.	
Κρυπτογράφηση	
	Κωδικοποίησε το μήνυμα ως m∈ R_p. Διάλεξε τυχαίο r∈T(d,d). Υπολόγισε $e(x) \equiv ph(x) * r(x) + m(x)\ (mod\ q)$.(κρυπτοκείμενο)
Αποκρυπτογράφηση	
Υπολόγισε a(x)=f(x)*e(x) $\equiv pg(x) * r(x) + f(x) * m(x)$ Μετέφερε το a(x) στο R και υπολόγισε $m \equiv F_p(x) * a(x)(mod\ p)$	

Το μέγεθος τόσο του ιδιωτικού όσο και του δημόσιου κλειδιού είναι O(n).Η πιο χρονοβόρα διαδικασία τόσο στην κρυπτογράφηση, όσο και στην αποκρυπτογράφηση είναι τα διάφορα γινόμενα (συνελίξεις) που γενικά θέλουν $O(n^2)$ πολλαπλασιασμούς. Ας παρατηρήσουμε όμως εδώ ότι επειδή όλα τα γινόμενα περιλαμβάνουν και τριαδικά πολυώνυμα, ουσιαστικά χρειαζόμαστε $O(n^2)$ προσθέσεις ή αφαιρέσεις. Επομένως χρειαζόμαστε $O(n^2)$ στοιχειώδη βήματα. Με άλλα λόγια η κρυπτογράφηση και η αποκρυπτογράφηση στο NTRU είναι πολύ γρήγορες.

Το πρόβλημα στο οποίο βασίζεται το NTRU μπορεί να διατυπωθεί ως εξής:
Δοθέντος του h(x) (που είναι το δημόσιο κλειδί) βρείτε τριαδικά πολυώνυμα f(x) και g(x) τέτοια ώστε $f(x) * h(x) \equiv g(x)(mod\ q)$.
Βλέπουμε ότι το πρόβλημα αυτό δεν έχει μοναδική λύση γιατί αν (f(x),g(x)) είναι μια λύση του, τότε και η $(x^k*f(x),x^k*g(x))$ είναι μία λύση, για $0 \le k < N$. Το πολυώνυμο $x^k*f(x)$ λέγεται περιστροφή (rotation) του f(x) γιατί με τη συνέλιξη, οι συντελεστές του έχουν περιστραφεί κυκλικά κατά k θέσεις. Επομένως, το $x^k*f(x)$ είναι και αυτό ένα ιδιωτικό κλειδί που δίνει το $x^k*m(x)$, δηλαδή το μήνυμα περιστρεμμένο κυκλικά κατά k θέσεις.

Σύμφωνα με όσα έχουμε αναφέρει για τα κρυπτοσυστήματα δημοσίου κλειδιού, το πρόβλημα στο οποίο βασίζεται το NTRU πρέπει να είναι υπολογιστικά δύσκολο για να είναι το κρυπτοσύστημα ασφαλές. Όπως το θέσαμε δεν φαίνεται αν είναι όντως δύσκολο υπολογιστικά. Θα δείξουμε όμως ότι ισοδυναμεί με την επίλυση του SVP σε μια ειδική κατηγορία πλεγμάτων, και επομένως μπορούμε να βασίσουμε το κρυπτοσύστημα σε αυτό το πρόβλημα. Ξεκινάμε ορίζοντας το πλέγμα που θα χρησιμοποιήσουμε το οποίο θα ονομάζουμε NTRU-πλέγμα.
Έστω $h(x)=h_o+h_1x+\ldots+h_{n-1}x^{n-1}$ ένα δημόσιο κλειδί στο NTRU. Το NTRU-πλέγμα L_h^{NTRU} που σχετίζεται με το h(x) είναι το πλέγμα διάστασης 2N που παράγεται από τις γραμμές του πίνακα

$$M_h^{NTRU}=\begin{pmatrix} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{pmatrix}$$

ο οποίος χωρίζεται σε τέσσερεις NxN υποπίνακες:
ο πάνω αριστερά που είναι ο μοναδιαίος πίνακας
ο κάτω αριστερά που είναι ο μηδενικός πίνακας
ο πάνω δεξιά που είναι οι συντελεστές του h(x) κυκλικά περιστραμμένοι
ο κάτω δεξιά που είναι ο μοναδιαίος πίνακας πολλαπλασιασμένος επί q.
Δηλαδή $M_h^{NTRU}=\begin{pmatrix} I & h \\ 0 & qI \end{pmatrix}$.
Έστω δύο πολυώνυμα $a(x)=a_o+a_1x+\ldots+a_{N-1}x^{N-1}$ και $b(x)=b_0+b_1x+\ldots+b_{N-1}x^{N-1}$.Το διάνυσμα $(a,b)=(a_o,a_1,\ldots,a_{N-1},b_0,b_1,\ldots,b_{N-1}) \in Z^{2N}$,που έχει δηλαδή στοιχεία τους συντελεστές των πολυωνύμων, αντιστοιχεί σε αυτά τα πολυώνυμα στο Z^{2N}.

Πρόταση 5.6) Έστω ότι $f(x) * h(x) \equiv g(x) (\mathrm{mod}\ q)$, και u(x) το πολυώνυμο που ικανοποιεί την $f(x) * h(x) = g(x) + qu(x)$.Τότε (f,-u) M_h^{NTRU}=(f,g) δηλαδή το (f,g) ανήκει στο L_h^{NTRU}.

Απόδειξη

Πράγματι (f,-u) M_h^{NTRU}=(f,-u) $\begin{pmatrix} I & h \\ 0 & qI \end{pmatrix}$=(f,f*h-qu)=(f,g)

Καταλήξαμε λοιπόν στο ότι το ιδιωτικό κλειδί (f,g) είναι ένα διάνυσμα στο Z^{2N} που ανήκει στο L_h^{NTRU}.Θα δείξουμε ότι είναι πολύ μικρό διάνυσμα και πιθανότατα το μικρότερο.

Πρόταση)Έστω (N,p,q,d) οι παράμετροι του NTRU για τις οποίες για απλοποίηση δεχόμαστε ότι ισχύουν $d \approx N/3$ και $q \approx 6d \approx 2N$.Τότε ισχύουν τα ακόλουθα
α)$\det(L_h^{NTRU})=q^N$.
β)$||(f,g)|| \approx \sqrt{4d} \approx \sqrt{4N/3} \approx 1.155\sqrt{N}$
γ)$\frac{||(f,g)||}{\sigma(L)}=O(1/\sqrt{N})$
Απόδειξη

α) $\det(L_h^{NTRU})=\det(M_h^{NTRU})=q^N$ γιατί είναι άνω τριγωνικός.

β) Εξ'ορισμού το f έχει d+1 συντελεστές ίσους με 1,d ίσους με -1 και το g d ίσους με 1 και d ίσους με -1.

γ) Γνωρίζουμε ότι $\sigma(L_h^{NTRU}) \approx \sqrt{\frac{Nq}{\pi e}} \approx 0.484N$.Άρα $\frac{||(f,g)||}{\sigma(L)} \approx \frac{2.39}{\sqrt{N}} = O(1/\sqrt{N})$.
Επομένως όσο μεγαλώνει το N το (f,g) γίνεται μικρότερο από το $\sigma(L_h^{NTRU})$.Δηλαδή για μεγάλα N αναμένουμε το μικρότερο μη μηδενικό διάνυσμα στο L_h^{NTRU} να είναι το (f,g) και οι περιστροφές του. Συνεπώς επιλύοντας το SVP για το L_h^{NTRU} βρίσκουμε το ιδιωτικό κλειδί (f,g) και άρα το αρχικό μας πρόβλημα ανάγεται στο SVP για τα πλέγματα της μορφής L_h^{NTRU}.

Κλείνουμε την παρουσίαση του NTRU με ένα μικρό παράδειγμα.

Παράδειγμα NTRU

Έστω ότι έχουμε τις παραμέτρους (N,p,q,d)=(7,3,41,2).Καταρχήν παρατηρούμε ότι (6d+1)p=(6*2+1)*3=39<41=q δηλαδή οι παράμετροι είναι καλά ορισμένες. Η Alice διαλέγει $f(x)=x^6-x^4x^3+x^2-1 \in T(3,2)$ και $g(x)=x^6+x^4-x^2-x \in T(2,2)$.Στη συνέχεια υπολογίζει τους αντιστρόφους $F_q(x)=f^{-1}(x) \bmod q=$
$8x^6+26x^5+31x^4+21x^3+40x^2+2x+37 \in R_q$ και
$F_p(x)=f^{-1}(x) \bmod p = x^6+2x^5+x^3+x^2+x+1 \in R_p$.Για το δημόσιο κλειδί της υπολογίζει το $h(x)=F_q(x)*g(x)=20x^6+40x^5+2x^4+38x^3+8x^2+26x+30 \in R_q$.

Ο Bob θέλει να στείλει το μήνυμα $m(x)=-x^5+x^3+x^2-x+1$ και διαλέγει το τυχαίο $r(x)=x^6-x^5+x-1$. Υπολογίζει λοιπόν το κρυπτοκείμενο
$e(x) \equiv ph(x) * r(x) + m(x) \ (mod\ q) \equiv 31x^6+19x^5+4x^4+2x^3+40x^2+3x+25 \pmod{41}$.

Η Alice για να το αποκρυπτογραφήσει υπολογίζει πρώτα το
$f(x)*e(x) \equiv x^6+10x^5+33x^4+40x^3+40x^2+x+40 \pmod{41}$ το οποίο μεταφέρει (centered lift) στο R και παίρνει $a(x)=x^6+10x^5-8x^4-x^3-x^2+x-1 \in R$.Στη συνέχεια υπολογίζει το $F_p(x)*a(x) \equiv 2x^5+x^3+x^2+2x+1 \pmod 3$ και κάνοντας το centered lift στο R ανακτά το αρχικό μήνυμα $m(x)= -x^5+x^3+x^2-x+1$.
Ας δούμε τώρα πως η Eve μπορεί χρησιμοποιώντας τον αλγόριθμο LLL να βρει το ιδιωτικό κλειδί της Alice δηλαδή να σπάσει το κρυπτοσύστημα. Καταρχήν σχηματίζει τον

$$M_h^{NTRU} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 30 & 26 & 8 & 38 & 2 & 40 & 20 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 20 & 30 & 26 & 8 & 38 & 2 & 40 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 40 & 20 & 30 & 26 & 8 & 38 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 40 & 20 & 30 & 26 & 8 & 38 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 38 & 2 & 40 & 20 & 30 & 26 & 8 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 8 & 38 & 2 & 40 & 20 & 30 & 26 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 26 & 8 & 38 & 2 & 40 & 20 & 30 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 41 \end{pmatrix}$$

Εφαρμόζοντας τον αλγόριθμο LLL παίρνουμε τον πίνακα

$M_{LLL}=$

$$\begin{pmatrix} 1 & 0 & -1 & 1 & 0 & -1 & -1 & -1 & 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & -1 & 0 & 1 & -1 & -1 & -1 & 0 & 1 & 0 & 1 & 0 \\ -1 & 1 & 0 & -1 & -1 & 1 & 0 & -1 & 0 & 1 & 1 & 0 & -1 & 0 \\ -1 & -1 & 1 & 0 & -1 & 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 & 1 \\ -1 & 1 & 0 & -1 & 1 & 0 & -1 & 0 & -1 & 0 & -1 & 0 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 & 1 & -1 & -1 & 0 & 0 & 2 & 0 & 0 \\ -8 & -1 & 0 & 9 & 0 & -1 & 0 & -4 & 2 & 6 & 0 & -4 & 7 & -7 \\ 8 & 1 & 0 & 0 & -8 & -1 & 2 & 0 & -5 & 8 & -7 & -3 & 1 & 6 \\ 0 & -9 & -2 & 1 & 9 & -1 & 0 & -6 & -3 & 2 & 5 & 0 & -5 & 7 \\ 0 & 8 & 0 & -9 & -1 & -8 & 8 & 2 & 7 & -11 & 3 & -5 & 2 & 2 \\ 1 & 0 & 0 & 9 & 2 & -1 & -9 & 5 & -7 & 6 & 3 & -2 & -5 & 0 \\ -2 & 1 & 9 & -1 & 0 & 0 & -9 & 2 & 5 & 0 & -5 & 7 & -6 & -3 \\ 3 & 2 & 3 & 3 & -6 & 2 & -6 & 11 & 6 & 8 & 0 & 9 & 5 & 2 \end{pmatrix}$$

Όπως πάντα παρατηρούμε ότι $H(M_h^{NTRU})=0.1184$ ενώ $H(M_{LLL})=0.8574$ δηλαδή εφαρμόζοντας τον αλγόριθμο πήραμε έναν πίνακα πολύ πιο κοντά στο να είναι ορθογώνιος. Το μικρότερο διάνυσμα είναι η πρώτη γραμμή του M_{LLL} και χωρίζοντας το ανά N=7 στοιχεία παίρνουμε τα πολυώνυμα $f'(x)=1-x^2+x^3-x^5-x^6$ και $g'(x)=-1-x^2+x^4+x^5$.Τα πολυώνυμα αυτά αποτελούν περιστροφές των αρχικών f(x) και g(x) ($f'(x)=-x^3*f(x)$ και $g'(x)=-x^3*g(x)$) και όπως έχουμε αναφέρει μπορούν να χρησιμοποιηθούν για αποκρυπτογράφηση.

Βιβλιογραφία

1)Θεωρία αριθμών και Κρυπτογραφία . Αλέξανδρος Παπαιωάννου

2) Σημειώσεις στη θεωρία αριθμών και την Κρυπτογραφία, Ε.Ζάχος

3)An introduction to Mathematical Cryptography, Jeffrey Hoffstein,Jill Pipher, Joseph H.Silverman .Springer 2008

4)Modern Cryptography, Wenbo Mao, Prentice Hall 2004

5) Complexity Theory and Cryptography ,Jorg Rothe, Springer 2004.