«ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ»

«Μεταπτυχιακές Σπουδές στα Μαθηματικά»

Δ Ι Π Λ Ω Μ Α Τ Ι Κ Η Ε Ρ Γ Α Σ Ι Α

«ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΓΡΑΜΜΙΚΗΣ ΑΛΓΕΒΡΑΣ ΣΤΗ ΘΕΩΡΙΑ ΤΩΝ ΑΛΥΣΙΔΩΝ MARKOV, ΣΤΗ ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ ΚΑΙ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ »

ΦΩΤΕΙΝΗ ΣΤΑΝΗΜΕΡΑΚΗ

ΑΜ 142652

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ

ΜΙΧΑΗΛ ΑΝΟΥΣΗΣ

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2022

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΦΑΡΜΟΓΕΣ ΤΗΣ ΓΡΑΜΜΙΚΗΣ ΑΛΓΕΒΡΑΣ ΣΤΗ ΘΕΩΡΙΑ ΤΩΝ ΑΛΥΣΙΔΩΝ MARKOV, ΣΤΗ ΘΕΩΡΙΑ ΤΩΝ ΠΑΙΓΝΙΩΝ ΚΑΙ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

ΦΩΤΕΙΝΗ ΣΤΑΝΗΜΕΡΑΚΗ

ΑΜ 142652

ΕΠΙΤΡΟΠΗ ΕΠΙΒΛΕΨΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΜΙΧΑΗΛ ΑΝΟΥΣΗΣ
ΚΑΘΗΓΗΤΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΥΝ-ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:
ΕΥΓΕΝΙΟΣ ΑΥΓΕΡΙΝΟΣ
ΚΑΘΗΓΗΤΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΑΘΗΝΑ

ΣΕΠΤΕΜΒΡΙΟΣ 2022

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσια του Μεταπτυχιακού Προγράμματος Σπουδών ≪Μεταπτυχιακές σπουδές στα Μαθηματικά≫ της Σχολής Θετικών Επιστημών και Τεχνολογίας του Ελληνικού Ανοικτού Πανεπιστημίου.

Θα ήθελα να ευχαριστήσω θερμά τον Α΄ Επιβλέποντα της παρούσας διπλωματικής εργασίας , καθηγητή του Πανεπιστημίου Αιγαίου, κ. Μιχαήλ Ανούση για τη στήριξη του καθώς χωρίς τη συνεχή ενθαρυνσή του , τις πολύτιμες οδηγίες του και τις επιστημονικές υποδείξεις του θα ήταν αδύνατη η εκπόνηση της.

Επίσης θα ήθελα να ευχαριστήσω εκ των προτέρων τον Β΄ Επιβλέποντα, καθηγητή του Πανεπιστημίου Αιγαίου, κ. Ευγένιο Αυγερινό για την τιμή που μου έκανε να αξιολογήσει την παρούσα διπλωματική εργασία.

Τέλος θα ήθελα να ευχαριστήσω την οικογένεια μου που ήταν δίπλα μου όλο αυτόν τον καιρό συμπαραστάτες στην προσπάθεια μου.

Στον σύζυγό μου

Στα παιδιά μου

Περίληψη

Η παρούσα διπλωματική έχει στόχο, μέσα από την υπάρχουσα βιβλιογραφία, να δούμε κάποιες εφαρμογές της γραμμικής άλγεβρας κυρίως σε άλλες επιστήμες. Το αντικείμενο είναι μελέτη μοντέλων και προβλημάτων από επιστήμες όπως η οικονομία , η γενετική , η κρυπτογραφία , θεωρία παιγνίων κ.τ.λ.

Σε ένα τυπικό μάθημα Γραμμικής Άλγεβρας όπου τα βάρος δίνεται στη μελέτη των αξιωμάτων και των θεωρημάτων και στις βασικές εφαρμογές τους δεν απομένει χρόνος για περισσότερες εφαρμογές πλέον των απαραίτητων.

Σε αυτή τη διπλωματική θα προσπαθήσουμε να γεφυρώσουμε το χάσμα ανάμεσα στα θεωρητικά μαθηματικά και στις εφαρμογές τους στις σύγχρονες επιστήμες όπως οι αλυσίδες Markov στην Οικονομία στη Γενετική στην Οικολογία, η Θεωρία παιγνίων στην Οικονομία και η Κρυπτογραφία στην Πληροφορική κ.λπ.

Στο πρώτο κεφάλαιο μελετάμε τη θεωρία των αλυσίδων Markov τους ορισμούς του πίνακα πιθανοτήτων, το διάνυσμα αρχικών πιθανοτήτων , τις χρονικά εξαρτημένες πιθανότητες τις οριακές καταστάσεις πιθανοτήτων και την ταξινόμηση των καταστάσεων μιας αλυσίδας Markov. Επίσης θα δούμε εφαρμογές των αλυσίδων Markov με συγκεκριμένα παραδείγματα.

Στο δεύτερο κεφάλαιο μελετάμε την κρυπτογραφία , έναν επιστημονικό κλάδο ύψιστης σημασίας στους τομείς της ασφάλειας υπολογιστικών συστημάτων και επικοινωνιών.

Θα δούμε τους ορισμούς της κρυπτογράφησης , της αποκρυπτογράφησης και της κρυπτανάλυσης και τις μεθόδους κατανόησης αυτών καθώς και τις σχετικές εφαρμογές.

Στο τρίτο κεφάλαιο ασχολούμαστε με τη θεωρία παιγνίων , τους ορισμούς παιγνίων με μηδενικό άθροισμα κέρδους – ζημιάς, την εύρεση βέλτιστης στρατηγικής και τις αντίστοιχες εφαρμογές.

Λέξεις – Κλειδιά

Αλυσίδα Markov, Πίνακας Μετάβασης ενός βήματος της αλυσίδας Markov, Χρονικά Εξαρτημένες πιθανότητες, Διάνυσμα αρχικών πιθανοτήτων, απορροφητική κατάσταση, παροδική κατάσταση, κρυπτογράφημα Hill, κρυπτογράφηση, αποκρυπτογράφηση, κρυπτανάλυση, αριθμητική υπολοίπων, παίγνιο, βέλτιστη στρατηγική, σαγματικό σημείο.

«Applications of Linear Algebra to the theory of Markov Chains, to Game theory and to Cryptography»

«Fotini Stanimeraki»

Abstract

The current thesis, through current bibliography, aims to see some applications of linear algebra mainly in other sciences. The object is a study of models and problems from sciences such as economics, genetics, cryptography, game theory, etc.

In a typical course of Linear Algebra where the emphasis is placed on the study of axioms and theorems and their basic applications there is no time left for more applications beyond the necessary. In this thesis we will try to bridge the gap between theoretical mathematics and their applications in modern sciences such as Cryptography in computer science, Markov chains in Economics in Genetics in Ecology, game theory in Economics and Cryptography in Informatics , etc.

In the first chapter we study the theory of the Markov chains the definitions of the probability table, the initial probability vector, the time-dependent probabilities, the boundary states of probability and the classification of the states of a Markov chain. We will also look at applications of Markov chains with specific examples.

In the second chapter we study cryptography, a scientific discipline of paramount importance in the fields of computer systems and communications security. We will look at the definitions of encryption, decryption and cryptanalysis and the methods of understanding them as well as the related applications.

In the third chapter we deal with game theory and discuss optimal strategy and applications.

Keywords

Markov chains, one-step transition table of the Markov chain, Time-dependent probabilities, Initial Probability Vector, absorbent state, transient state, Hill cipher, encryption, decryption, cryptanalysis, balance arithmetic, play, optimal strategy, saddle point.

Περιεχόμενα

Περίληψη v
Abstract vii
Περιεχόμενα ix
Κατάλογος Εικόνων / Σχημάτων xi
Κατάλογος Πινάκων xii
Συντομογραφίες & Ακρωνύμια xiii
Κεφάλαιο 1 Αλυσίδες Markov 1
1.1 Αλυσίδα Markov 1
1.2 Πίνακας Μετάβασης ενός βήματος της αλυσίδας Markov. 1
1.2.1 Παραδείγματα: 2
1.3 Χρονικά Εξαρτημένες πιθανότητες. 3
1.3.1 Ορισμός 6
1.3.2 Θεώρημα Chapman – Kolmogorov: 6
1.4 Διάνυσμα αρχικών πιθανοτήτων 6
1.4.1 Θεώρημα 7
1.4.2 Συμπεράσματα: 7
1.5 Οριακές Πιθανότητες των καταστάσεων 9
1.5.1 Ορισμός : 12
1.5.2 Τυχαίος περίπατος 13
1.5.3 Εργοδικό Σύστημα: 13
1.6 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΚΑΤΑΣΤΑΣΕΩΝ ΜΙΑΣ ΑΛΥΣΙΔΑΣ MARKOV 14
1.6.1 Ορισμός : 14
1.6.2 Πρόταση : 14
1.6.3 Ορισμός : 14
1.6.4 Ορισμός : 15
1.6.5 Γενίκευση 18
1.7 ΕΠΑΝΟΔΟΣ ΚΑΙ ΠΑΡΟΔΙΚΟΤΗΤΑ. 19
1.7.1 Ορισμός : 19
1.7.2 Θεώρημα (Πρώτης εισόδου) 19
1.7.3 Λήμμα : 20
1.7.4 Θεώρημα (Τύπος του Doeblin) 20
1.7.5 Πόρισμα : 20
1.7.6 Πόρισμα : 20
1.7.7 Πόρισμα : 21
1.7.8 Πόρισμα : 21
1.7.9 Θεώρημα : 21
1.8 Εφαρμογές: 26
1.8.1 Εφαρμογή 26
1.8.2 Εφαρμογή 28
2 ΚΕΦΑΛΑΙΟ 2 ΚΡΥΠΤΟΓΡΑΦΙΑ 30
2.1 ΚΡΥΠΤΟΓΡΑΦΙΑ: 30
2.2 ΙΣΤΟΡΙΚΗ ΑΝΑΦΟΡΑ 30

2.3 ΟΡΙΣΜΟΙ....32
2.4 ΚΡΥΠΤΟΓΡΑΦΗΜΑΤΑ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ....33
2.5 ΠΟΛΥΓΡΑΦΙΚΟ ΣΥΣΤΗΜΑ....33
2.6 ΚΡΥΠΤΟΓΡΑΦΗΜΑ HILL....34
2.7 Modular Arithmetic –Αριθμητική Υπολοίπων....36
2.7.1 Ορισμός....36
2.7.2 Θεώρημα :....37
2.8 ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ....39
2.8.1 Ορισμός....39
2.8.2 Ορισμός....39
2.8.3 Θεώρημα :....41
2.8.4 Πόρισμα :....41
2.8.5 Πόρισμα :....41
2.9 ΚΡΥΠΤΑΝΑΛΥΣΗ....44
2.9.1 Θεώρημα : Καθορισμός του πίνακα αποκρυπτογράφησης.....45
2.10 ΕΦΑΡΜΟΓΕΣ....48
2.10.1 Εφαρμογή :....48
2.10.2 Εφαρμογή :....50
2.10.3 Εφαρμογή :....51
3 ΚΕΦΑΛΑΙΟ ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ....54
3.1 Εισαγωγή....54
3.1.1 Παίγνιο....55
3.2 Παίγνιο δύο ατόμων με μηδενικό άθροισμα κέρδους- ζημιάς.....56
3.2.1 Ορισμός....56
3.2.2 Ορισμός 57
3.2.3 Ορισμός 58
3.2.4 Παράδειγμα....58
3.3 Παίγνια με επιλογή στρατηγικής.....59
3.3.1 Θεώρημα:....59
3.3.2 Ορισμός 60
3.4 Εύρεση βέλτιστης στρατηγικής με χρήση Σαγματικού Σημείου.....61
3.4.1 Ορισμός 61
3.4.2 Παράδειγμα.....62
3.4.3 Παράδειγμα Βέλτιστες στρατηγικές για την μεγιστοποίηση της τηλεθέασης. 63
3.5 Εύρεση βέλτιστης στρατηγικής με χρήση πίνακα 2×2.....64
3.5.1 Θεώρημα 65
3.5.2 Εφαρμογή....66
Βιβλιογραφία....69

Κατάλογος Εικόνων / Σχημάτων

Εικόνα 1 Δεντροδιάγραμμα 4
Εικόνα 2 Τροχονόμος 11
Εικόνα 3 Κρύπτεια σκυτάλη 31
Εικόνα 4 Μηχανή Enigma 32
Εικόνα 5 Παίγνιο 1 55

Κατάλογος Πινάκων

Πίνακας 1 Πιθανότητες καταστάσεων συστήματος 2- θέσεων 5
Πίνακας 2 Παράδειγμα 6 10
Πίνακας 3 Παράδειγμα 7 12
Πίνακας 4 Πίνακας κρυπτογραφήματος Hill 34
Πίνακας 5 Αντίστροφοι modulo26 40
Πίνακας 6 Πληρωμή στον παίκτη Α 55
Πίνακας 7 Πίνακας τηλεθέασης 63

Συντομογραφίες & Ακρωνύμια

Κεφάλαιο 1 Αλυσίδες Markov

1.1 Αλυσίδα Markov

Υποθέστε, ότι ένα μαθηματικό σύστημα υφίσταται μια διαδικασία αλλαγής τέτοια ώστε κάθε στιγμή μπορεί να λάβει μία από ένα πεπερασμένο πλήθος επιλογών. Για παράδειγμα ο καιρός σε μια συγκεκριμένη πόλη μπορεί να είναι νεφελώδης, ηλιόλουστος ή βροχερός. Ή ένα άτομο μπορεί να έχει μια από τις παρακάτω συναισθηματικές καταστάσεις , χαρούμενο , λυπημένο, θυμωμένο ή αγχωμένο. Υποθέστε ότι αυτό το σύστημα αλλάζει από τη μία θέση στην άλλη με το χρόνο και σε συγκεκριμένες στιγμές το παρατηρούμε. Εάν η κατάσταση του συστήματος σε κάθε παρατήρηση δεν μπορεί να προβλεφθεί με ακρίβεια , αλλά η πιθανότητα να προκύψει η συγκεκριμένη κατάσταση απλά ξέροντας την προηγούμενη κατάσταση είναι γνωστή τότε η διαδικασία της αλλαγής ονομάζεται Αλυσίδα Markov ή διαδικασία Markov. (Markov chain)

Δηλαδή **αλυσίδα Markov**, ή **Μαρκοβιανή αλυσίδα**, που πήρε το όνομα της από τον Andrey Markov, είναι ένα μαθηματικό σύστημα που μεταβάλλεται από μια κατάσταση σε μια άλλη, ανάμεσα σε ένα αριθμό καταστάσεων. Είναι μια τυχαία διαδικασία που δε διατηρεί μνήμη για τις προηγούμενες μεταβολές, η επόμενη κατάσταση εξαρτάται μόνο από την τωρινή κατάσταση και σε καμιά περίπτωση από αυτές που προηγήθηκαν. Αυτό το συγκεκριμένο είδος "αμνησίας" ονομάζεται Μαρκοβιανή ιδιότητα. Οι Μαρκοβιανές Αλυσίδες έχουν πολλές εφαρμογές ως στατιστικά μοντέλα καθημερινών διαδικασιών.

1.2 Πίνακας Μετάβασης ενός βήματος της αλυσίδας Markov.

Εάν μια αλυσίδα Markov έχει k πιθανές επιλογές τότε η πιθανότητα ότι το σύστημα είναι στη θέση i ενώ ήταν στη θέση j στην προηγούμενη παρατήρηση υποδηλώνεται ως p_{ij} και καλείται μεταβατική πιθανότητα ή πιθανότητα μετάβασης από τη θέση j στη θέση i. Ο πίνακας P=[p_{ij}] ονομάζεται Πίνακας Μετάβασης ενός βήματος της αλυσίδας Markov. Για παράδειγμα σε μια αλυσίδα Markov 3 επιλογών ο πίνακας Μετάβασης ενός βήματος έχει αυτή τη μορφή:

Προηγούμενη κατάσταση

$$\begin{matrix} & 1 & 2 & 3 & \\ \end{matrix}$$
$$\begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix} \begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$$

Καινούργια κατάσταση

Σε αυτόν τον πίνακα το στοιχείο p_{32} είναι η πιθανότητα ότι το σύστημα μεταβάλλεται από την κατάσταση 2 στην κατάσταση 3, p_{11} είναι η πιθανότητα ότι το σύστημα θα παραμείνει στη θέση 1 εάν πριν ήταν στη θέση 1.

1.2.1 **Παραδείγματα:**

Παράδειγμα 1 *:*

Ένα γραφείο ενοικιάσεων αυτοκινήτων έχει 3 περιοχές ενοικίασης αεροδρόμιο, λιμάνι, κέντρο. Ένας πελάτης μπορεί να παραλάβει το αυτοκίνητο σε οποιαδήποτε από τις τρεις περιοχές και να το επιστρέψει σε οποιαδήποτε από τις τρεις. Ο υπεύθυνος διαπιστώνει ότι ο πελάτης επιστρέφει το αυτοκίνητο στις πιθανές τοποθεσίες σύμφωνα με τις παρακάτω πιθανότητες.

Παραλαβή από τοποθεσία

	Αεροδρόμιο	Λιμάνι	Κέντρο	
	0,8	0,3	0,2	*Αεροδρόμιο*
	0,1	0,2	0,6	*Λιμάνι*
	0,1	0,5	0,2	*Κέντρο*

Επιστροφή σε τοποθεσία

Αυτός ο πίνακας είναι ένας πίνακας μετάβασης της αλυσίδας Markov. Από αυτόν τον πίνακα καταλαβαίνουμε ότι η πιθανότητα ένας πελάτης να παρέλαβε από το κέντρο και να επέστρεψε το αυτοκίνητο στο λιμάνι είναι 0,6, ενώ η πιθανότητα να παρέλαβε από το αεροδρόμιο και να το επέστρεψε στο αεροδρόμιο είναι 0,8.

Παράδειγμα 2:

Ελέγχοντας τα αρχεία δωρεών ένας υπεύθυνος μιας εκκλησίας ανακαλύπτει ότι το 80% των πιστών οι οποίοι συνεισφέρουν μια χρονιά συνεισφέρουν και την επόμενη και το 30% αυτών που δεν συνεισφέρουν τη μια χρονιά, δωρίζουν την επόμενη. Αυτό μπορεί να φανεί ως αλυσίδα Markov με 2 επιλογές. Επιλογή 1 ο πιστός δίνει δωρεά , επιλογή 2 , δεν δίνει. Ο πίνακας μετάβασης ενός βήματος της αλυσίδας Markov είναι ο παρακάτω.

$$\begin{bmatrix} 0,8 & 0,3 \\ 0,2 & 0,7 \end{bmatrix}$$

Στα παραπάνω παραδείγματα οι πίνακες Μετάβασης των αλυσίδων Markov έχουν την ιδιότητα ότι το άθροισμα της κάθε στήλης είναι 1. Αυτό δεν είναι τυχαίο . Εάν P=[p_{ij}] είναι ο πίνακας μετάβασης μιας αλυσίδας Markov με k επιλογές, για κάθε j πρέπει να έχουμε: $p_{1j} + p_{2j} + p_{3j} + \cdots + p_{kj} = 1$ διότι εάν το σύστημα είναι στη θέση j σε μια παρατήρηση είναι βέβαιο ότι θα είναι σε μια από τις k πιθανές θέσεις στην επόμενη παρατήρηση.
Ένας πίνακας με αυτήν την ιδιότητα καλείται **Στοχαστικός πίνακας** ή **πίνακας πιθανοτήτων** ή **πίνακας** Markov. Από τα παραπάνω καταλαβαίνουμε ότι ένας πίνακας Μετάβασης ενός βήματος της αλυσίδας Markov πρέπει να είναι ένας Στοχαστικός πίνακας

1.3 Χρονικά Εξαρτημένες πιθανότητες.

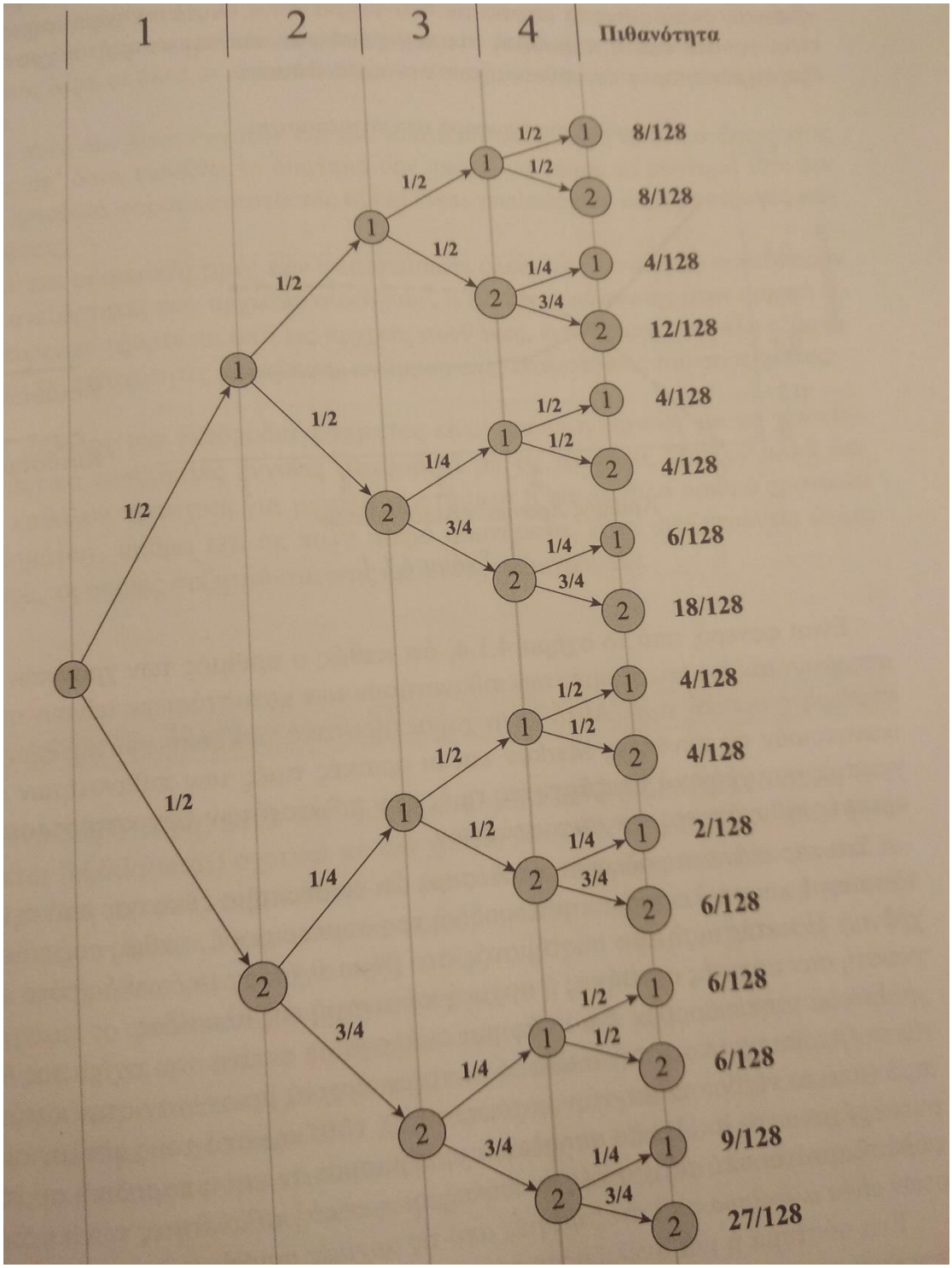
Για να υπολογίσουμε την παροδική συμπεριφορά ενός συστήματος χρησιμοποιώντας τον πίνακα μετάβασης ενός βήματος, ας δούμε το παρακάτω παράδειγμα,

Παράδειγμα 3

Έχουμε ένα απλό σύστημα δύο καταστάσεων με πίνακα μετάβασης ενός βήματος.

$$P=\begin{bmatrix} \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & \frac{3}{4} \end{bmatrix}$$

Θεωρούμε ότι το σύστημα είναι αρχικά στη θέση 1 , στο πρώτο διάστημα χρόνου το σύστημα μπορεί παραμείνει στη θέση 1 με πιθανότητα $\frac{1}{2}$ ή να μετακινηθεί στη θέση 2 με πιθανότητα $\frac{1}{2}$. Όταν το σύστημα είναι στη θέση 2 μπορεί να μετακινηθεί στη θέση 1 με πιθανότητα $\frac{1}{4}$ ή να παραμείνει στην ίδια θέση με πιθανότητα $\frac{3}{4}$.
Ένας από τους τρόπους με τους οποίους μπορεί να γίνει διαισθητικά φανερή η συμπεριφορά αυτού του συστήματος είναι με τη βοήθεια του δεντροδιαγράμματος που φαίνεται στην εικόνα 1.



Εικόνα 1 Δεντροδιάγραμμα

Υποθέτοντας ότι το σύστημα ξεκινά από τη θέση 1 , το παραπάνω διάγραμμα δείχνει τις θέσεις στις οποίες μπορεί να βρίσκεται το σύστημα μετά από κάθε βήμα ή χρονικό διάστημα μέχρι και τέσσερα τέτοια χρονικά διαστήματα.
Η πιθανότητα του να ακολουθεί κανείς , κάποιο κλάδο αυτού του δένδρου μπορεί να υπολογιστεί πολλαπλασιάζοντας τις αντίστοιχες πιθανότητες αυτού του κλάδου. Ακόμα η πιθανότητα του να βρίσκεται το σύστημα σε μια συγκεκριμένη θέση μετά από συγκεκριμένο αριθμό βημάτων υπολογίζεται προσθέτοντας τις πιθανότητες των κλάδων που οδηγούν σε αυτή τη θέση. Οι πιθανότητες των κλάδων φαίνονται επίσης στο σχήμα 2 για τη θέση που εμφανίζεται μετά από τέσσερα χρονικά διαστήματα.
Εάν όλες οι πιθανότητες προστεθούν , πάλι θα βρεθεί ότι το άθροισμα τους είναι ίσο με τη μονάδα.. Έτσι η πιθανότητα του να βρίσκεται το σύστημα στη θέση 1 μετά από τέσσερα βήματα είναι $\frac{43}{128}$ ενώ η πιθανότητα να είναι στη θέση 2 είναι $\frac{85}{128}$.
Χρησιμοποιώντας την ίδια τεχνική για τον υπολογισμό των πιθανοτήτων των κλάδων και των πιθανοτήτων των θέσεων μετά από κάθε χρονικό διάστημα παίρνουμε τον παρακάτω πίνακα:

Πίνακας 1 Πιθανότητες καταστάσεων συστήματος 2- θέσεων

Πιθανότητες καταστάσεων συστήματος 2-θέσεων.

Χρονικό διάστημα	Θέση 1	Θέση 2
1	$\frac{1}{2} = 0{,}5$	$\frac{1}{2} = 0{,}5$
2	$\frac{3}{8} = 0{,}375$	$\frac{5}{8} = 0{,}625$
3	$\frac{11}{32} = 0{,}344$	$\frac{21}{32} = 0{,}656$
4	$\frac{43}{128} = 0{,}336$	$\frac{85}{128} = 0{,}664$

Εάν πολλαπλασιάσουμε τον πίνακα με τον εαυτό του, παίρνουμε:

$$P^{(2)} = \begin{bmatrix} p_{11}^{(2)} & p_{12}^{(2)} \\ p_{21}^{(2)} & p_{22}^{(2)} \end{bmatrix} = P \cdot P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} \cdot \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix} = \begin{bmatrix} \frac{3}{8} & \frac{5}{16} \\ \frac{5}{8} & \frac{11}{16} \end{bmatrix}$$

Το πρώτο στοιχείο της πρώτης γραμμής , $p_{11}^{(2)}$είναι η πιθανότητα να είμαστε στην κατάσταση 1 μετά από δύο χρονικά διαστήματα δοθέντος ότι ξεκινήσαμε από τη θέση 1.
Όμοια το 2ο στοιχείο της πρώτης στήλης. $p_{21}^{(2)}$ είναι η πιθανότητα να είμαστε στην θέση 2 μετά από 2 χρονικά διαστήματα δοθέντος ότι ξεκινήσαμε στη θέση 1. Ανάλογα είναι τα αποτελέσματα για τη 2η στήλη.
Εάν οι τιμές της 1ης στήλης συγκριθούν με αυτές του πίνακα 1 παρατηρούμε ότι ταυτίζονται με τις πιθανότητες που υπολογίζονται μετά από δύο χρονικά διαστήματα δοθέντος ότι το σύστημα ξεκίνησε από τη θέση 1.
Έτσι τελικά τα στοιχεία του πίνακα $P^{(2)}$ δίνουν όλες τις πιθανότητες μετάβασης για ένα σύστημα 2 καταστάσεων μετά από δύο χρονικά διαστήματα.
Αυτό μπορεί να γενικευτεί για κάθε δύναμη του πίνακα P και για μια οποιαδήποτε αλυσίδα Markov.

1.3.1 **Ορισμός**

Ορίζουμε τον πίνακα $P^{(n)} = \left[p_{x,y}^{(n)}\right]$ όπου $p_{x,y}^{(n)}$ παριστάνει την πιθανότητα να βρίσκεται το σύστημα στη θέση x μετά από ν χρονικά διαστήματα, δοθέντος ότι ξεκίνησε από τη θέση y. **Ο πίνακας $P^{(n)}$ καλείται πίνακας μετάβασης ν βημάτων της αλυσίδας.**

1.3.2 **Θεώρημα Chapman – Kolmogorov:**

$\forall$ x, y ϵ S, n, m =1,2,… $p_{x,y}^{(n+m)} = \sum_{z \in S} p_{x,z}^{(n)} \, p_{z,y}^{(m)}$

Με τη βοήθεια των πινάκων μετάβασης η παραπάνω ισότητα γίνεται

$$P^{(n+m)} = P^{(n)} \cdot P^{(m)}$$

και ακόμη παρατηρώντας ότι

$$P^{(2)} = P^{(1)} \cdot P^{(1)} = P \cdot P = P^2$$

οπότε επαγωγικά παίρνουμε

$$P^{(n)} = P^n \qquad \text{n= 1,2,…}$$

Δηλαδή για να υπολογίσουμε τον πίνακα μετάβασης n-βημάτων αρκεί να υπολογίσουμε τη n-ιοστή δύναμη του πίνακα P , δηλαδή τον πίνακα P^n

1.4 Διάνυσμα αρχικών πιθανοτήτων

Πολλές φορές εκτός από τις παραπάνω δεσμευμένες πιθανότητες θα θέλαμε να υπολογίσουμε τις πιθανότητες να βρισκόμαστε σε μια συγκεκριμένη θέση κάποια συγκεκριμένη χρονική στιγμή. Σε μια αλυσίδα Markov η κατάσταση του συστήματος σε κάθε παρατήρηση γενικά δεν μπορεί να αποφασιστεί με βεβαιότητα . Το καλύτερο που μπορούμε να κάνουμε να ορίσουμε πιθανότητες για κάθε μια από τις πιθανές επιλογές. Για παράδειγμα σε μια αλυσίδα Markov με τρείς επιλογές μπορούμε να περιγράψουμε την πιθανή κατάσταση του συστήματος σε κάποια παρατήρηση από το παρακάτω διάνυσμα στήλη στο οποίο x_1 είναι η πιθανότητα της επιλογής 1, x_2 είναι η πιθανότητα της επιλογής 2 και x_3 είναι η πιθανότητα της επιλογής 3.

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

Το διάνυσμα θέσης για κάθε παρατήρηση σε μια αλυσίδα Markov με k δυνατές επιλογές είναι ένα διάνυσμα στήλη του οποίου το i στοιχείο x_i είναι η πιθανότητα ότι το σύστημα είναι στην i επιλογή αυτή τη στιγμή. Παρατηρούμε ότι οι καταχωρήσεις σε οποιοδήποτε διάνυσμα θέσης για μια αλυσίδα Markov είναι μη αρνητικές και έχουν άθροισμα 1. Ένα διάνυσμα στήλη το οποίο έχει αυτήν την ιδιότητα ονομάζεται **Διάνυσμα αρχικών Πιθανοτήτων**.

1.4.1 **Θεώρημα**

Εάν P είναι ο πίνακας μετάβασης μιας αλυσίδας Markov και $x^{(n)}$ είναι το διάνυσμα θέσης στη νιοστή παρατήρηση τότε αποδεικνύεται ότι $x^{(n+1)} = P \cdot x^{(n)}$

Άμεση συνέπεια αυτού του θεωρήματος είναι ότι

$x^{(1)}=P \cdot x^{(0)}$
$x^{(2)}=P \cdot x^{(1)}=P \cdot P \cdot x^{(0)}$
$x^{(3)}=P \cdot x^{(2)}=P \cdot P^{2} \cdot x^{(0)}$
…….
$x^{(n)}=P \cdot x^{(n-1)}=P^{n} \cdot x^{(0)}$

Έτσι βλέπουμε ότι η νιοστή παρατήρηση εξαρτάται από τον πίνακα μετάβασης και το αρχικό διάνυσμα θέσης.

1.4.2 **Συμπεράσματα:**

Μια αλυσίδα Markov καθορίζεται μονοσήμαντα από τη αρχική της κατάσταση και τον πίνακα Μετάβασης ενός βήματος. Ισχύει και το αντίστροφο , εάν δοθεί ένα αρχικό διάνυσμα και ένας πίνακας μετάβασης ενός βήματος, τότε υπάρχει μια αλυσίδα Markov με αρχικό διάνυσμα και πίνακας μετάβασης ενός βήματος τα δοθέντα.
Οι πιθανότητες των καταστάσεων μπορούν να υπολογιστούν σε κάθε χρονικό διάστημα απλά πολλαπλασιάζοντας το διάνυσμα θέσης της αρχικής κατάστασης με τον πίνακα μετάβασης ενός βήματος με τον εαυτό του τον αντίστοιχο αριθμό φορών. Οι οριακές πιθανότητες των καταστάσεων μπορούν να υπολογιστούν συνεχίζοντας τον πολλαπλασιασμό για κατάλληλο αριθμό φορών.

Παράδειγμα 4

Ένα άτομο πουλάει το αυτοκίνητό του κάθε χρόνο και αγοράζει ένα καινούργιο . Εάν έχει ένα Citroen το πουλάει και αγοράζει ένα Opel . Εάν έχει ένα Opel το πουλάει και αγοράζει ένα Fiat. Όμως εάν έχει ένα Fiat ,όταν το πουλήσει είναι εξίσου πιθανό να αγοράσει είτε ένα Citroen είτε ένα Opel. Το 2022 αγόραζει ένα Fiat. Τι πιθανότητα έχει να έχει το 2024 ένα Fiat ή ένα Citroen;
Η παραπάνω διαδικασία μπορεί να περιγραφή με μια τη βοήθεια μιας αλυσίδας Markov με πίνακα μετάβασης ενός βήματος τον παρακάτω:

Αυτοκίνητο που πουλάει

$$P = \begin{matrix} C & O & F \end{matrix} \begin{bmatrix} 0 & 0 & \frac{1}{2} \\ 1 & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{bmatrix} \begin{matrix} C \\ O \\ F \end{matrix}$$

Αυτοκίνητο που αγοράζει

Το 2022(αρχή των χρόνων) αγοράζει ένα Fiat δηλαδή το διάνυσμα θέσης της αρχικής κατάστασης είναι

$$X = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \begin{matrix} C \\ O \\ F \end{matrix}$$

Οι πιθανότητες για το τι τύπου αυτοκίνητο θα έχει το 2024 (δύο χρόνια μετά το 2022) δίνονται από τη σχέση:

$$X^{(2)} = P^2 \cdot X = \begin{bmatrix} 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} \\ 1 & 0 & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \begin{matrix} C \\ O \\ F \end{matrix}$$

Δηλαδή η πιθανότητα το 2024 να έχει ένα Opel είναι 50% , ένα Fiat 50%, ενώ ένα Citroen είναι 0%.

1.5 Οριακές Πιθανότητες των καταστάσεων

Παράδειγμα 5:

Στο παράδειγμα 2 είχαμε τον πίνακα μετάβασης $P=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}$.

Τώρα κατασκευάζουμε την πιθανότητα μελλοντικής δωρεάς για έναν πιστό που δεν έδωσε δωρεά τον πρώτο χρόνο. Τότε το διάνυσμα θέσης είναι $x^{(0)}=\begin{bmatrix}0\\ 1\end{bmatrix}$

Από το Θεώρημα 2.4.1 έχουμε:

$$x^{(1)}=P\cdot x^{(0)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0\\ 1\end{bmatrix}=\begin{bmatrix}0,3\\ 0,7\end{bmatrix}$$

$$x^{(2)}=P\cdot x^{(1)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,3\\ 0,7\end{bmatrix}=\begin{bmatrix}0,45\\ 0,55\end{bmatrix}$$

$$x^{(3)}=P\cdot x^{(2)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,45\\ 0,55\end{bmatrix}=\begin{bmatrix}0,525\\ 0,475\end{bmatrix}$$

Έτσι μετά από 3 χρόνια περιμένουμε ο πιστός να κάνει δωρεά με πιθανότητα 0,525. Μετά τα 3 χρόνια βρίσκουμε τα παρακάτω διανύσματα θέσης:

$$x^{(4)}=P\cdot x^{(3)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,525\\ 0,475\end{bmatrix}=\begin{bmatrix}0,563\\ 0,438\end{bmatrix}$$

$$x^{(5)}=P\cdot x^{(4)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,563\\ 0,438\end{bmatrix}=\begin{bmatrix}0,581\\ 0,419\end{bmatrix}$$

$$x^{(6)}=P\cdot x^{(5)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,581\\ 0,419\end{bmatrix}=\begin{bmatrix}0,591\\ 0,409\end{bmatrix}$$

$$x^{(7)}=P\cdot x^{(6)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\left[\begin{bmatrix}0,591\\ 0,409\end{bmatrix}\right]=\begin{bmatrix}0,595\\ 0,405\end{bmatrix}$$

$$x^{(8)}=P\cdot x^{(7)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,595\\ 0,405\end{bmatrix}=\begin{bmatrix}0,598\\ 0,402\end{bmatrix}$$

$$x^{(9)}=P\cdot x^{(8)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,598\\ 0,402\end{bmatrix}=\begin{bmatrix}0,599\\ 0,401\end{bmatrix}$$

$$x^{(10)}=P\cdot x^{(9)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,599\\ 0,401\end{bmatrix}=\begin{bmatrix}0,599\\ 0,401\end{bmatrix}$$

$$x^{(9)}=P\cdot x^{(8)}=\begin{bmatrix}0,8 & 0,3\\ 0,2 & 0,7\end{bmatrix}\cdot\begin{bmatrix}0,599\\ 0,401\end{bmatrix}=\begin{bmatrix}0,600\\ 0,400\end{bmatrix}$$

Για όλα τα n>11 έχουμε $x^{(n)}=\begin{bmatrix}0,600\\0,400\end{bmatrix}$ με προσέγγιση 3 δεκαδικών ψηφίων. Με άλλα λόγια το διάνυσμα θέσης συγκλίνει σε ένα συγκεκριμένο διάνυσμα όσο μεγαλώνει ο αριθμός των παρατηρήσεων.

Παράδειγμα 6:

Ας ξαναπάμε στο παράδειγμα 1:

Ο πίνακας Μετάβασης στο παράδειγμα 1 ήταν ο εξής:

$P=\begin{bmatrix}0,8 & 0,3 & 0,2\\0,1 & 0,2 & 0,6\\0,1 & 0,5 & 0,2\end{bmatrix}$ εάν ένα αυτοκίνητο αρχικά ενοικιάστηκε στη θέση 2 Λιμάνι τότε το αρχικό διάνυσμα θέσης είναι $x^{(0)}=\begin{bmatrix}0\\1\\0\end{bmatrix}$ χρησιμοποιώντας αυτό το διάνυσμα και το Θεώρημα 2.4.1 έχουμε τον παρακάτω πίνακα:

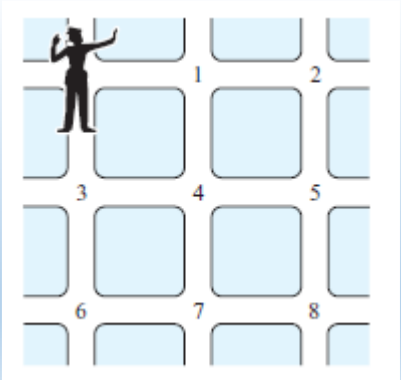
Πίνακας 2 Παράδειγμα 6

	0	1	2	3	4	5	6	7	8	9	10	11
$x_1^{(n)}$	0	0,300	0,400	0,477	0,511	0,533	0,544	0,550	0,553	0,555	0,556	0,557
$x_2^{(n)}$	1	0,200	0,370	0,252	0,261	0,240	0,238	0,233	0,232	0,233	0,230	0,230
$x_3^{(n)}$	0	0,500	0,230	0,271	0,228	0,227	0,219	0,217	0,215	0,214	0,214	0,213

Δύο πράγματα μπορούμε να παρατηρήσουμε στο παράδειγμα 6. Πρώτον ότι δεν χρειάζεται να ξέρουμε πόσο καιρό ο πελάτης κράτησε το αυτοκίνητο. Δεύτερον το διάστημα θέσης προσεγγίζει ένα συγκεκριμένο διάνυσμα όσο αυξάνεται, όπως και στο προηγούμενο παράδειγμα.

Παράδειγμα 7: (Χρησιμοποιώντας το Θεώρημα 1.4.1)

Μία τροχονόμος ρυθμίζει την κυκλοφορία σε 8 διασταυρώσεις όπως φαίνεται στην εικόνα 2. Οι οδηγίες που έχει είναι, να παραμείνει στην κάθε διασταύρωση για μια ώρα και μετά είτε να παραμείνει στην ίδια διασταύρωση είτε να μετακινηθεί σε μια διπλανή διασταύρωση. Για να αποφύγει την δημιουργία μοτίβου, της έχουν πει να διαλέγει την καινούρια διασταύρωση σε τυχαία βάση με κάθε δυνατή επιλογή ισοπίθανη. Για παράδειγμα εάν είναι στη διασταύρωση 5 ,η επόμενη επιλογή μπορεί να είναι η 2,η 4, η 5,ή η 8 η κάθε μία με πιθανότητα $\frac{1}{4}$. Κάθε ημέρα ξεκινάει στην τοποθεσία στην οποία σταμάτησε την προηγούμενη.



Εικόνα 2 Τροχονόμος

Ο πίνακας μετάβασης για αυτήν την αλυσίδα Markov είναι:

Παλιά διασταύρωση

	1	2	3	4	5	6	7	8	
1	$\frac{1}{3}$	$\frac{1}{3}$	0	$\frac{1}{5}$	0	0	0	0	1
2	$\frac{1}{3}$	$\frac{1}{3}$	0	0	$\frac{1}{4}$	0	0	0	2
3	0	0	$\frac{1}{3}$	$\frac{1}{5}$	0	$\frac{1}{3}$	0	0	3
4	$\frac{1}{3}$	0	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{1}{4}$	0	$\frac{1}{4}$	0	4
5	0	$\frac{1}{3}$	0	$\frac{1}{5}$	$\frac{1}{4}$	0	0	$\frac{1}{3}$	5
6	0	0	$\frac{1}{3}$	0	0	$\frac{1}{3}$	$\frac{1}{4}$	0	6
7	0	0	0	$\frac{1}{5}$	0	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{3}$	7
8	0	0	0	0	$\frac{1}{4}$	0	$\frac{1}{4}$	$\frac{1}{3}$	8

Νέα διασταύρωση

Εάν η τροχονόμος ξεκινήσει στη διασταύρωση 5,οι πιθανές τις τοποθεσίες , ώρα με την ώρα, δίνονται από τα διανύσματα θέσεις στον πίνακα 3. Για όλες τις τιμές για n > 22, όλα τα διανύσματα θέσης προσεγγίζουν το $x^{(22)}$ με προσέγγιση τριών δεκαδικών ψηφίων. Συνεπώς όπως και στα δύο πρώτα παραδείγματα, το διάνυσμα θέσης προσεγγίζει κάποιο σταθερό διάνυσμα όσο αυξάνεται το n.

Πίνακας 3 Παράδειγμα 7

n	0	1	2	3	4	5	10	15	20	22
$x_1^{(n)}$	0	0	0,133	0,116	0,130	0,123	0,113	0,109	0,108	0,107
$x_2^{(n)}$	0	0,250	0,146	0,163	0,140	0,138	0,115	0,109	0,108	0,107
$x_3^{(n)}$	0	0	0,050	0,039	0,067	0,073	0,100	0,106	0,107	0,107
$x_4^{(n)}$	0	0,250	0,113	0,187	0,162	0,178	0,178	0,179	0,179	0,179
$x_5^{(n)}$	1	0,250	0,279	0,190	0,190	0,168	0,149	0,144	0,143	0,143
$x_6^{(n)}$	0	0	0,000	0,050	0,056	0,074	0,099	0,105	0,107	0,107
$x_7^{(n)}$	0	0	0,133	0,104	0,131	0,125	0,138	0,142	0,143	0,143
$x_8^{(n)}$	0	0,250	0,146	0,152	0,124	0,121	0,108	0,107	0,107	0,107

Στα παραδείγματα είδαμε ότι το διάνυσμα θέσης προσεγγίζει κάποιο σταθερό διάνυσμα όσο ο αριθμός των παρατηρήσεων αυξάνεται. Το ερώτημα μας τώρα είναι αν το διάνυσμα θέσης προσεγγίζει πάντα ένα σταθερό διάνυσμα σε μια αλυσίδα Markov.

Αυτό δεν ισχύει πάντα και αυτό φαίνεται στο παρακάτω παράδειγμα.

Παράδειγμα 8:

Το σύστημα ταλαντεύεται ανάμεσα σε δύο διανύσματα θέσης:

Έστω $P = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ και $x^{(0)} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ τότε $P^2 = I$ και $P^3 = P$ και $x^{(0)} = x^{(2)} = x^{(4)} = \ldots = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ενώ $x^{(1)} = x^{(3)} = x^{(5)} = \ldots = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ το σύστημα ταλαντεύεται ανάμεσα στα διανύσματα $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ και $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ έτσι δεν συγκλίνει σε κανένα. Παρ ’όλα αυτά εάν εισάγουμε μια ήπια προϋπόθεση μπορούμε να δείξουμε ότι ένα σταθερό διάνυσμα θέσης μπορεί να προσεγγιστεί. Αυτή η προϋπόθεση περιγράφεται με τον ακόλουθο ορισμό.

1.5.1 **Ορισμός :**

Ένας πίνακας Μετάβασης είναι **κανονικός** εάν έχει όλες τις καταχωρήσεις του *θετικές*. Δηλαδή για έναν κανονικό πίνακα μετάβασης P , υπάρχει κάποιος φυσικός αριθμός m τέτοιος ώστε όλες οι καταχωρήσεις του P^m είναι θετικές, δηλαδή δεν υπάρχει μηδενική καταχώρηση.

Έτσι στα παραδείγματα 1 και 2 ο πίνακας είναι κανονικός για m=1 ενώ στο παράδειγμα 5 ο P^4 έχει όλες τις καταχωρήσεις θετικές.

Μια αλυσίδα Markov η οποία έχει έναν κανονικό πίνακα καλείται **Κανονική Αλυσίδα Markov.** Θα δούμε ότι κάθε κανονική αλυσίδα Markov έχει ένα σταθερό διάνυσμα q τέτοιο ώστε $P^n \cdot x^{(0)}$προσεγγίζει το q όσο το n αυξάνεται, για οποιαδήποτε επιλογή του $x^{(0)}$.
Αυτό το συμπέρασμα είναι μέγιστης σημασίας στη θεωρία των αλυσίδων Markov.

1.5.2 Τυχαίος περίπατος.

Τυχαίος περίπατος είναι η κατάσταση κατά την οποία μπορεί να γίνει μόνο ένα βήμα μπροστά ή πίσω ή να παραμείνει στην ίδια θέση. Σε αυτή την περίπτωση οι πιθανότητες μετάβασης ενός βήματος γίνονται:

$$p_{ij} = \begin{cases} p & i = j+1 \\ q & i = j-1 \\ r & i = j \\ 0 & αλλού \end{cases}$$

Μια πιθανή ερμηνεία ενός τυχαίου περιπάτου είναι και η ακόλουθη: έστω ότι ένα σωματίδιο κινείται πάνω σε μια ευθεία κάνοντας ένα βήμα μπροστά ή ένα βήμα πίσω σε κάθε χρονική στιγμή ή παραμένει ακίνητο.

1.5.3 Εργοδικό Σύστημα:

Ένα σύστημα για το οποίο οι οριακές τιμές των πιθανοτήτων των θέσεων είναι ανεξάρτητες των αρχικών συνθηκών είναι γνωστό ως εργοδικό.
Για να είναι ένα σύστημα εργοδικό θα πρέπει κάθε θέση του συστήματος να είναι προσιτή από όλες τις άλλες θέσεις του συστήματος άμεσα ή έμμεσα. Δηλαδή θα πρέπει οι θέσεις να επικοινωνούν μεταξύ τους.
Εάν αυτό δεν είναι δυνατόν και σε μια ιδιαίτερη κατάσταση ή καταστάσεις στις οποίες εφόσον εισέλθει το σύστημα δεν μπορεί να φύγει , τότε το σύστημα δεν είναι εργοδικό και οι καταστάσεις αυτές είναι γνωστές σαν **απορροφητικές** καταστάσεις δηλαδή έχουν πιθανότητα 1.
Το πιο γνωστό παράδειγμα τυχαίου περιπάτου με απορροφητικές καταστάσεις είναι αυτό του παίχτη (gambler's ruin) .
Έστω ένας παίχτης με αρχικό κεφάλαιο X παίζει παιχνίδια ποντάροντας σε κάθε παιχνίδι ένα ευρώ. Έτσι στο τέλος κάθε γύρου έχει κερδίσει ένα ευρώ με πιθανότητα p ή έχει χάσει ένα ευρώ με πιθανότητα q. Εάν ο παίχτης παίζοντας τα παιχνίδια χάσει όλα του τα χρήματα αποχωρεί , όπως επίσης αποχωρεί εάν ποτέ κερδίσει ένα συγκεκριμένο ποσό b ευρώ. Άρα εδώ έχουμε απορροφητική κατάσταση στο 0 και στο b.

1.6 ΤΑΞΙΝΟΜΗΣΗ ΤΩΝ ΚΑΤΑΣΤΑΣΕΩΝ ΜΙΑΣ ΑΛΥΣΙΔΑΣ MARKOV

1.6.1 **Ορισμός :**

Θα λέμε ότι η κατάσταση x οδηγεί στην κατάσταση y, ή ότι η κατάσταση y είναι προσιτή από την κατάσταση x και θα γράφουμε x→y αν υπάρχει θετική πιθανότητα σε έναν πεπερασμένο αριθμό μεταβάσεων το σύστημα να κινηθεί από το x στο y , δηλαδή αν για κάποιο n≥0, $P^{(n)}(x, y) > 0$.

Αν x→ y και y→ x , θα λέμε ότι οι καταστάσεις επικοινωνούν και γράφουμε x↔y

1.6.2 **Πρόταση :**

Η σχέση επικοινωνίας είναι μια σχέση ισοδυναμίας στο χώρο των καταστάσεων S μιας αλυσίδας Markov.
Απόδειξη:

i) Η σχέση είναι ανακλαστική. Πράγματι, αν x ∈ S τότε x ↔ x γιατί $P^{(0)}(x, x) = 1$

ii) Η σχέση είναι συμμετρική δηλαδή αν x ↔ y τότε y↔ x προκύπτει άμεσα από τον ορισμό της επικοινωνίας.

iii) Η σχέση είναι επίσης μεταβατική γιατί, εάν x,y,z ∈S και έστω ότι x↔y και y↔z. Τότε υπάρχουν m,n ≥ 0 τέτοια ώστε $P^{(m)}(x, y) \cdot P^{(n)}(y, z) > 0$
Από τις σχέσεις Chapman- Kolmogorov, έχουμε:
$P^{(m+n)}(x, z) = \sum_{w \in S} P^{(m)}(x, w)\ P^{(n)}(w, z) \geq P^{(m)}(x, y)\ P^{(n)}(y, z) > 0$

άρα x →z και όμοια z→x δηλαδή x↔z.
Η σχέση δηλαδή της επικοινωνίας σαν σχέση ισοδυναμίας διαμερίζει τον χώρο καταστάσεων S σε *κλάσεις ισοδυναμίας* , δηλαδή σε ξένα μεταξύ τους σύνολα καταστάσεων, τα στοιχεία καθενός εκ των οποίων επικοινωνούν μεταξύ τους.

1.6.3 **Ορισμός :**

Ένα σύνολο καταστάσεων C⊆ S καλείται (στοχαστικά) ***κλειστό*** αν p(x,y) = 0, για όλα τα x ∈ C και για όλα τα y ∉ C, δηλαδή από τη στιγμή που το σύστημα εισέρχεται στο σύνολο C , παραμένει εκεί για πάντα.

Ένα κλειστό σύνολο C καλείται ***ανάγωγο*** αν συμπίπτει με μια κλάση ισοδυναμίας. Μια αλυσίδα Markov καλείται *ανάγωγη* αν ο χώρος καταστάσεων είναι ένα ανάγωγο σύνολο. Μια κατάσταση x καλείται ***απορροφητική*** εάν p(x,x) =1 , δηλαδή εάν το σύστημα εισέλθει στην x παραμένει εκεί για πάντα. Είναι φανερό ότι μια απορροφητική κατάσταση είναι ένα κλειστό ανάγωγο σύστημα.

1.6.4 **Ορισμός :**

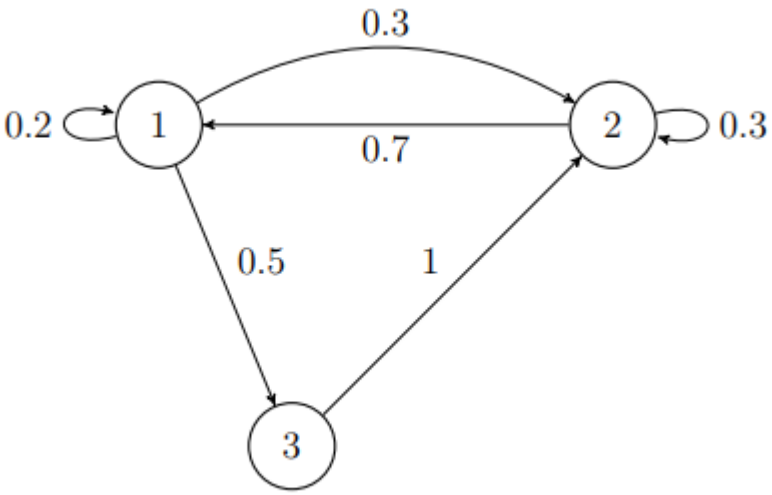
Θεωρούμε μια χρονικά ομογενή Αλυσίδα Markov με χώρο καταστάσεων S .
Το ***κατευθυνόμενο γράφημα της αλυσίδας*** είναι ένα γράφημα με κορυφές που αντιστοιχούν στα στοιχεία του S.
Αν x,y ∈ S τότε το γράφημα έχει μια ακμή που ξεκινάει από το x και καταλήγει στο y αν και μόνο αν $p(x,y) \neq 0$

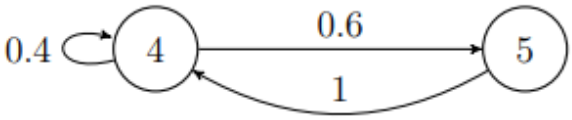
Παράδειγμα 9:

Εάν μια αλυσίδα Markov έχει τον παρακάτω πίνακα μετάβασης ενός βήματος:

$$P = \begin{bmatrix} 0.2 & 0.7 & 0 & 0 & 0 \\ 0.3 & 0.3 & 1 & 0 & 0 \\ 0.5 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0.4 & 1 \\ 0 & 0 & 0 & 0.6 & 0 \end{bmatrix}$$

Κατασκευάζοντας το κατευθυνόμενο γράφημα της αλυσίδας, δηλαδή ένα γράφημα το οποίο περιέχει τις καταστάσεις της αλυσίδας και τις αντίστοιχες πιθανότητες μετάβασης ενός βήματος ,έχουμε:





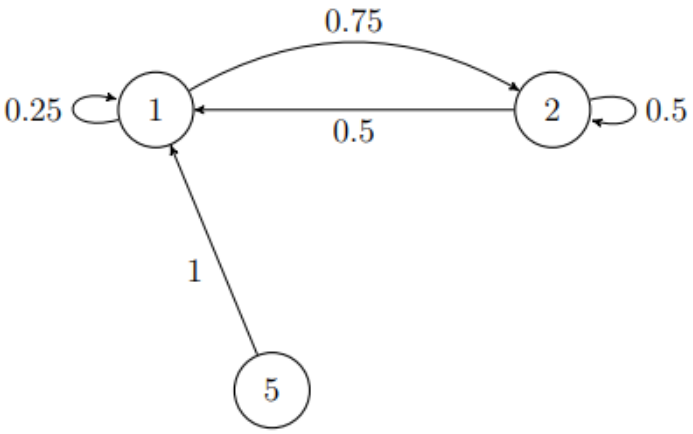
Βλέπουμε δηλαδή ότι ο χώρος καταστάσεων διαμερίζετε σε δύο κλάσεις ;
$C_1 = \{1,2,3\}$ και $C_2 = \{4,5\}$. Είναι φανερό ότι τα σύνολα αυτά είναι κλειστά.

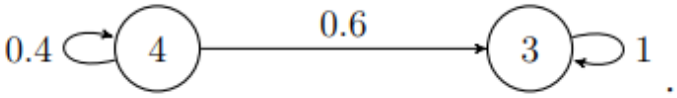
Παράδειγμα 10:

Εάν η αλυσίδα Markov έχει τον παρακάτω πίνακα μετάβασης

$$P = = \begin{bmatrix} 0.25 & 0.5 & 0 & 0 & 1 \\ 0.75 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0.6 & 0 \\ 0 & 0 & 0 & 0.4 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Με κατευθυνόμενο γράφημα





Οι κλάσεις ισοδυναμίας του χώρου καταστάσεων είναι $C_1 = \{1,2\}$, $C_2 = \{3\}$, $C_3 = \{4\}$, $C_4 = \{5\}$.
Τα σύνολα C_1 και C_2 είναι κλειστά ενώ τα C_3 και C_4 δεν είναι .
Η κατάσταση 3 είναι απορροφητική.

1.6.5 **Γενίκευση**

Τυχαίος περίπατος με φράγματα απορρόφησης στα 0,b .
Η αλυσίδα Markov έχει πίνακα μετάβασης ενός βήματος˝

$$P = \begin{array}{c} \begin{matrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \dots & \boldsymbol{b-1} & \boldsymbol{b} \end{matrix} \\ \begin{bmatrix} 1 & q & 0 & \dots & 0 & 0 \\ 0 & r & q & \dots & 0 & 0 \\ 0 & p & r & \dots & 0 & 0 \\ 0 & 0 & p & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & q & 0 \\ 0 & 0 & 0 & \dots & r & 0 \\ 0 & 0 & 0 & \dots & p & 1 \end{bmatrix} \end{array} \begin{matrix} \mathbf{0} \\ \mathbf{1} \\ \mathbf{2} \\ . \\ . \\ . \\ \boldsymbol{b-1} \\ \boldsymbol{b} \end{matrix}$$

Ο χώρος καταστάσεων αναλύεται στις κλάσεις {0},{1,2,3,…,b-1,b}, {b} όπου οι {0},{b} είναι κλειστά σύνολα. Οι καταστάσεις 0 και b είναι απορροφητικές.

1.7 ΕΠΑΝΟΔΟΣ ΚΑΙ ΠΑΡΟΔΙΚΟΤΗΤΑ.

Συχνά είναι χρήσιμο να ξέρουμε αν ένα σύστημα , ξεκινώντας από μια θέση x θα επιστρέψει κάποτε σε αυτήν την θέση ή όχι.
Με τη βοήθεια λοιπόν της έννοιας της επανόδου σε μια θέση , ορίζουμε μια δεύτερη κατάταξη των καταστάσεων-θέσεων της αλυσίδας.
Σε μια αλυσίδα Markov με χώρο καταστάσεων S, ορίζουμε τις ακόλουθες πιθανότητες.
Για καταστάσεις x, y και n≥1
f^n (x,y)= P{X_n = y, X_{n-1}≠y ,…,X_1≠y / X_0 = x}
είναι η δεσμευμένη πιθανότητα δεδομένου ότι το σύστημα ξεκίνησε από τη θέση x, η πρώτη μετάβαση στη θέση y να γίνει το χρόνο n.

Ακόμα με $f^*(x,y)$ συμβολίζουμε την πιθανότητα το σύστημα να επιστρέψει κάποτε στη κατάσταση y, δεδομένου ότι ξεκίνησε από την κατάσταση x. Δηλαδή την πιθανότητα , ξεκινώντας από τη κατάσταση x , υπάρχει μια χρονική στιγμή n κατά την οποία το σύστημα θα βρίσκεται στην κατάσταση y .
$f^*(x,y)$= P ($\cup_{n=1}^{\infty}${X_n=y/X_0=x})
Και αποδεικνύεται ότι:
$f^*(x,y)$= $\sum_{n=1}^{\infty} f^n$ (x, y)

1.7.1 **Ορισμός :**

Μια κατάσταση x∈S καλείται **επανερχόμενη** ή έμμονη αν $f^*(x,x)$=1, δηλαδή η x είναι επανερχόμενη αν με πιθανότητα 1 η Αλυσίδα Markov αρχίζοντας από τη x, θα επιστρέψει τελικά στη x, σε κάποια χρονική στιγμή.
Μια ειδική περίπτωση επανερχόμενης κατάστασης είναι και η **απορροφητική** (το ότι μια κατάσταση είναι απορροφητική , φαίνεται από την εμφάνιση ενός 1 στη διαγώνιο του πίνακα μετάβασης ενός βήματος).
Μια κατάσταση x∈S καλείται ***παροδική* ή *μεταβατική*** αν $f^*(x,x)$ <1.
Δηλαδή υπάρχει θετική πιθανότητα ίση με 1-$f^*(x,x)$, το σύστημα ξεκινώντας από την κατάσταση x να μην επιστρέψει ποτέ σε αυτήν.

1.7.2 **Θεώρημα (Πρώτης εισόδου)**

Για κάθε x,y∈S, n≥1 έχουμε:
$p^{(n)}$ (x , y) = $\sum_{m=1}^{n} f^{(n)}$(x, y) $p^{(n-m)}$(y, y)

1.7.3 **Λήμμα :**

Έστω $\{a_n\}_{n\geq 0}$ μια ακολουθία μη-αρνητικών πραγματικών αριθμών με $\sum_{n\geq 0} a_n < +\infty$
Έστω επίσης $\{b_n\}_{n\geq 0}$ μια πραγματική ακολουθία συγκλίνουσα στο b. Τότε:

$$b = \lim_{n\to\infty} \frac{\sum_{k=0}^{n} a_k b_{n-k}}{\sum_{k=0}^{n} a_k}$$

1.7.4 **Θεώρημα (Τύπος του Doeblin)**

Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S. Για κάθε x,y∈S έχουμε:

$$f^*(x,y) = \lim_{N\to\infty} \frac{\sum_{n=1}^{N} p^{(n)}(x,y)}{\sum_{n=0}^{N} p^{(n)}(y,y)}$$

1.7.5 **Πόρισμα :**

Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S.

- Μια κατάσταση x∈S είναι επανερχόμενη αν και μόνο αν η σειρά
  $\sum_{n=0}^{\infty} p^{(n)}(x,x)$ αποκλίνει.
- Μια κατάσταση x∈S είναι παροδική αν και μόνο αν η σειρά
  $\sum_{n=0}^{\infty} p^{(n)}(x,x)$ συγκλίνει.

1.7.6 **Πόρισμα :**

Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S. Έστω x∈S και y∈S μια παροδική κατάσταση. Τότε η σειρά

$$\sum_{n=1}^{\infty} p^{(n)}(x,y)$$

Συγκλίνει.

1.7.7 **Πόρισμα :**

Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S και A⊆S.Αν το A είναι πεπερασμένο και κλειστό, τότε το A έχει τουλάχιστον μια επανερχόμενη κατάσταση.

1.7.8 **Πόρισμα :**

Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S. Αν το S είναι πεπερασμένο τότε το S έχει μια τουλάχιστον επανερχόμενη κατάσταση.

1.7.9 **Θεώρημα :**

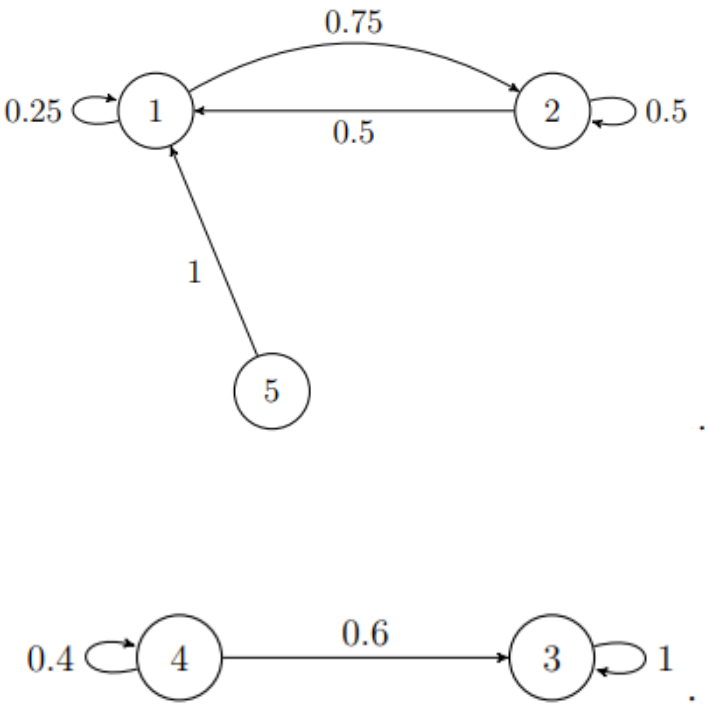
Έστω $\{X_n\}_{n\geq 0}$ αλυσίδα Markov με χώρο καταστάσεων S . Έστω x,y ∈S. Αν x↔y , τότε και οι δύο είναι επανερχόμενες ή και οι δύο είναι παροδικές.

Παράδειγμα 11:

Εάν μία Αλυσίδα Markov έχει πίνακα μετάβασης ενός βήματος:

$$P=\begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{array}\begin{array}{c} \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \end{array} \\ \begin{bmatrix} 0.25 & 0.5 & 0 & 0 & 1 \\ 0.75 & 0.5 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0.6 & 0 \\ 0 & 0 & 0 & 0.4 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Το κατευθυνόμενο γράφημα της αλυσίδας είναι:



Οι κλάσεις είναι: $C_1=\{1,2\}, C_2=\{3\}, C_3=\{4\}, C_4=\{5\}$

Η κλάση C_1 είναι σύνολο κλειστό και πεπερασμένο. Από το πόρισμα 2.7.8 έχει μία τουλάχιστον επανερχόμενη κατάσταση και επειδή είναι ανάγωγο (γιατί είναι μια κλάση ισοδυναμίας) , από το θεώρημα 2.7.9 όλες οι καταστάσεις στο {1,2} είναι επανερχόμενες.

Το ίδιο ισχύει και για το C_2 άρα και η κατάσταση 3 είναι επανερχόμενη.

Μάλιστα:
$f^*(3,3)= f^1(3,3)=1$
Η κατάσταση 3 είναι απορροφητική.

Η κατάσταση 4 είναι παροδική γιατί:
$f^*(4,4)= f^1(4,4)=0,4<1$

Η κατάσταση 5 είναι παροδική γιατί:
$f^*(5,5)=0<1$

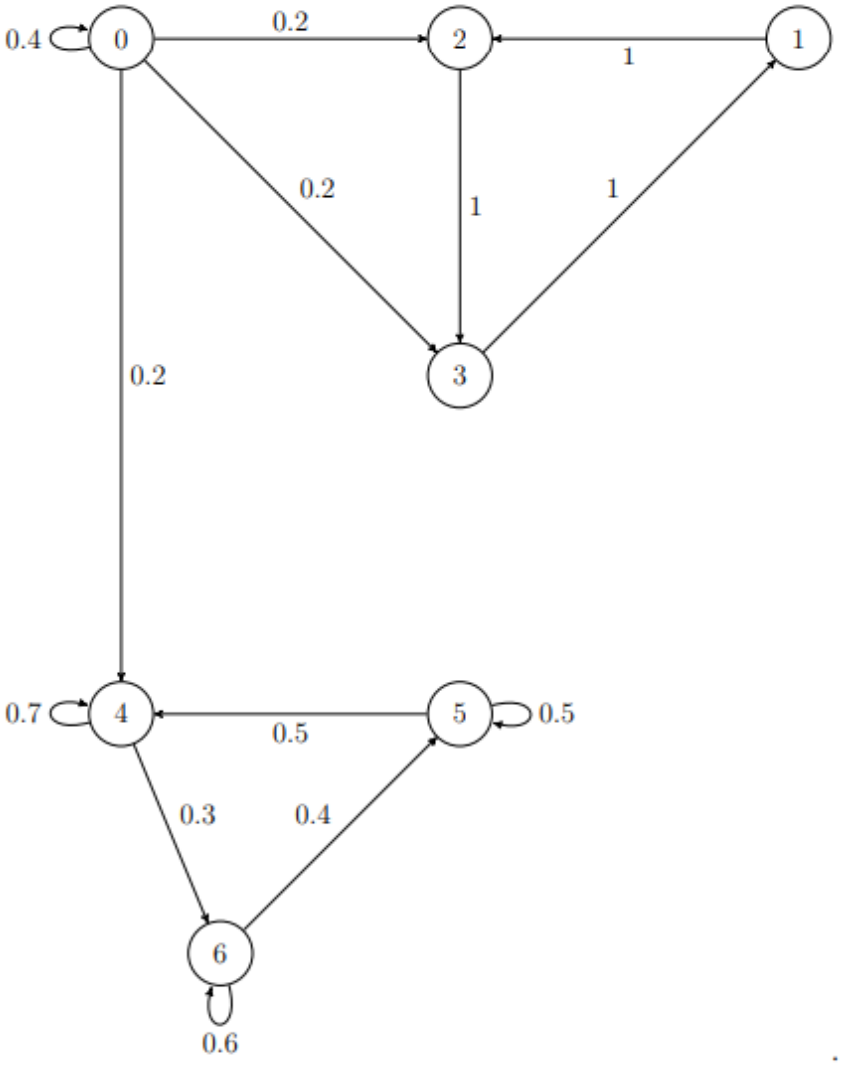
Παράδειγμα 12:

Έστω ότι έχουμε την αλυσίδα Markov με πίνακα μετάβασης:

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{array} \\ \begin{bmatrix} 0.4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0.2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0.2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0.2 & 0 & 0 & 0 & 0.7 & 0.5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0.5 & 0.4 \\ 0 & 0 & 0 & 0 & 0.3 & 0 & 0.6 \end{bmatrix} \end{array}$$

Οι κλάσεις ισοδυναμίας της αλυσίδας είναι $C_1=\{0\}$, $C_2=\{1,2,3\}$,$C_3=\{4,5,6\}$

Το κατευθυνόμενο γράφημα της αλυσίδας είναι:



Το σύνολο C_2 είναι κλειστό και πεπερασμένο άρα περιέχει μια επανερχόμενη κατάσταση και επειδή είναι ανάγωγο οι καταστάσεις 1,2,3 είναι επανερχόμενες..
Για τον ίδιο λόγο οι καταστάσεις 4,5,6 είναι επανερχόμενες.
Η κατάσταση 0 είναι παροδική γιατί $f^*(0,0)=0,4<1$

1.8 Εφαρμογές:

1.8.1 **Εφαρμογή**

Κάποιος πηγαίνει στη δουλειά του ή με το αυτοκίνητό του ή με το μετρό. Υποθέστε ότι ποτέ δεν παίρνει το μετρό δύο μέρες στη σειρά, αλλά εάν πάει στη δουλειά του με το αυτοκίνητα, τότε την επόμενη μέρα είναι εξίσου πιθανό να πάρει το μετρό ή το αυτοκίνητο. Μπορούμε να βρούμε :
α) Την πιθανότητα να πάει στη δουλειά του με το αυτοκίνητο μετά από δύο μέρες
β) Την πιθανότητα να πάει στη δουλειά του με το αυτοκίνητο μετά από δύο μέρες εάν την πρώτη μέρα εργασίας ρίχνει ένα συμμετρικό ζάρι και πηγαίνει με το αυτοκίνητο αν εμφανιστεί δύο.
Εδώ έχουμε δύο καταστάσεις ,την **0** και την **1** ,όπου
0=«το άτομο πηγαίνει στη δουλειά του με το αυτοκίνητο»
1=« το άτομο πηγαίνει στη δουλειά του με το μετρό»
Κάνοντας την υπόθεση «με τι μέσο πηγαίνει κάποιος στη δουλειά του μια μέρα γνωρίζοντας με τι μέσο πήγε την προηγούμενη μέρα και τις αμέσως προηγούμενες, εξαρτάται από το με τι μέσο πήγε στη δουλειά του την προηγούμενη μέρα» έχουμε μια αλυσίδα Markov.
Ο πίνακας μετάβασης ενός βήματος της αλυσίδας Markov είναι:

$$P = \begin{matrix} \\ \frac{1}{2} \\ \frac{1}{2} \end{matrix} \begin{matrix} 0 & 1 \\ 1 & \\ 0 & \end{matrix} \begin{matrix} \\ 0 \\ 1 \end{matrix}$$

α) Οι πιθανότητες μετάβασης μετά από δύο ημέρες , δηλαδή μετά από δύο χρονικά διαστήματα δίνεται από τον $P^{(2)} = P^2$

$$P^{(2)} = P^2 = P \cdot P = \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{2} & 1 \\ \frac{1}{2} & 0 \end{bmatrix} = \begin{matrix} 0 & 1 \\ \end{matrix} \begin{matrix} \\ \begin{bmatrix} \frac{3}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix} \end{matrix} \begin{matrix} \\ 0 \\ 1 \end{matrix}$$

Υποθέτουμε ότι την 1η μέρα πηγαίνει με το μετρό. Σε αυτήν την περίπτωση το διάνυσμα αρχικών πιθανοτήτων είναι

$$X(0) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

και οι πιθανότητες των καταστάσεων μετά από δύο μέρες είναι:

$$X(2) = P^{(2)} \cdot X(0) = P^2 \cdot X(0) = \begin{bmatrix} \frac{3}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{1}{2} \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix}$$

Δηλαδή αν πάει στη δουλειά την πρώτη μέρα με το μετρό , μετά από δύο μέρες χρησιμοποιεί ή το αυτοκίνητο ή το μετρό με την ίδια πιθανότητα.
Υποθέτουμε ότι την πρώτη μέρα χρησιμοποιεί το αυτοκίνητο ,τότε το αρχικό διάνυσμα πιθανοτήτων είναι

$$X(0) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

και

$$X(2) = P^{(2)} \cdot X(0) = P^2 \cdot X(0) = \begin{bmatrix} \frac{3}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{3}{4} \\ \frac{1}{4} \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix}$$

Δηλαδή η πιθανότητα να πάρει το αυτοκίνητο είναι τρεις φορές μεγαλύτερη από το να πάρει το μετρό.

β) Η πιθανότητα να φέρουμε 2 σε μια απλή ρίψη ενός συμμετρικού ζαριού είναι $\frac{1}{6}$. Έτσι το διάνυσμα των αρχικών πιθανοτήτων είναι

$$X(0) = \begin{bmatrix} \frac{1}{6} \\ \frac{5}{6} \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix}$$

και

$$X(2) = P^{(2)} \cdot X(0) = P^2 \cdot X(0) = \begin{bmatrix} \frac{3}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{6} \\ \frac{5}{6} \end{bmatrix} = \begin{bmatrix} \frac{13}{24} \\ \frac{11}{24} \end{bmatrix} \begin{matrix} 0 \\ 1 \end{matrix}$$

Άρα η πιθανότητα να χρησιμοποιήσει το αυτοκίνητο για να πάει στη δουλειά του δύο μέρες αργότερα είναι $\frac{13}{24}$.

1.8.2 **Εφαρμογή**

Ένας πωλητής αυτοκινήτων έχει συμβόλαιο για τρεις πόλεις: την Θεσσαλονίκη, την Καβάλα και την Ξάνθη. Είναι γνωστό ότι δεν μένει στην ίδια πόλη δύο ημέρες συνεχόμενες. Εάν επισκέπτεται τη Θεσσαλονίκη, τότε την επόμενη μέρα επισκέπτεται την Καβάλα. Εάν όμως επισκέπτεται την Καβάλα ή την Ξάνθη, τότε την επόμενη μέρα η πιθανότητα να επισκεφτεί την Θεσσαλονίκη είναι διπλάσια από το επισκεφτεί την άλλη πόλη. Μακροπρόθεσμα πόσο συχνά επισκέπτεται κάθε πόλη;

Η παραπάνω διαδικασία μπορεί να περιγραφεί με τη βοήθεια μιας αλυσίδας Markov, όπου η τυχαία μεταβλητή X_n= παριστάνει **την πόλη στην οποία βρίσκεται ο πωλητής τη n-οστή μέρα.**
Οι τρεις καταστάσεις της εν λόγω αλυσίδας συμβολίζονται με Θ, Κ, Ξ και ορίζονται ως εξής:

Θ = « Ο πωλητής βρίσκεται στην πόλη Θεσσαλονίκη»
Κ= « Ο πωλητής βρίσκεται στην πόλη Καβάλα»
Ξ = « Ο πωλητής βρίσκεται στην πόλη Ξάνθη »

Ο πίνακας μετάβασης ενός βήματος της αλυσίδας Markov είναι ίσος με:

$$P = \begin{matrix} \\ \Theta \\ K \\ \Xi \end{matrix} \begin{matrix} \begin{matrix} \Theta & K & \Xi \end{matrix} \\ \begin{bmatrix} 0 & \frac{2}{3} & \frac{2}{3} \\ 1 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 \end{bmatrix} \end{matrix}$$

Γιατί p(Θ,Θ)=p(Κ,Κ)=p(Ξ,Ξ)= 0 γιατί ο πωλητής δεν μένει στην δύο μέρες συνεχόμενες στη ίδια πόλη.
Ακόμη p(Κ,Θ)=$\frac{2}{3}$ και p(Κ,Ξ)=$\frac{1}{3}$, γιατί όταν βρίσκεται στην Καβάλα , η πιθανότητα να πάει στη Θεσσαλονίκη είναι διπλάσια από την πιθανότητα να πάει στην Ξάνθη.
Όμοια p(Ξ,Θ)=$\frac{2}{3}$ και p(Ξ,Κ)=$\frac{1}{3}$, γιατί όταν βρίσκεται στην Ξάνθη , η πιθανότητα να πάει στη Θεσσαλονίκη είναι διπλάσια από την πιθανότητα να πάει στην Καβάλα.

Το πόσο συχνά επισκέπτεται την κάθε πόλη μακροπρόθεσμα , δίνεται από το διάνυσμα οριακών πιθανοτήτων των καταστάσεων Θ,Κ,Ξ. Έχουμε λοιπόν:

$$P\cdot\begin{bmatrix} x_\Theta \\ x_K \\ x_\Xi \end{bmatrix} = \begin{bmatrix} x_\Theta \\ x_K \\ x_\Xi \end{bmatrix} \Rightarrow \begin{bmatrix} 0 & \frac{2}{3} & \frac{2}{3} \\ 1 & 0 & \frac{1}{3} \\ 0 & \frac{1}{3} & 0 \end{bmatrix} \cdot \begin{bmatrix} x_\Theta \\ x_K \\ x_\Xi \end{bmatrix} = \begin{bmatrix} x_\Theta \\ x_K \\ x_\Xi \end{bmatrix}$$

$$\Rightarrow\begin{cases} 0\cdot x_{\Theta}+\frac{2}{3}\cdot x_{K}+\frac{2}{3}\cdot x_{\Xi}=x_{\Theta} \\ 1\cdot x_{\Theta}+0\cdot x_{K}+\frac{1}{3}\cdot x_{\Xi}=x_{K} \\ 0\cdot x_{\Theta}+\frac{1}{3}\cdot x_{K}+0\cdot x_{\Xi}=x_{\Xi} \end{cases}\Rightarrow\begin{cases} \frac{2}{3}\cdot x_{K}+\frac{2}{3}\cdot x_{\Xi}=x_{\Theta} \\ x_{\Theta}+\frac{1}{3}\cdot x_{\Xi}=x_{K} \\ \frac{1}{3}\cdot x_{K}=x_{\Xi} \end{cases}$$

Απαλείφοντας μια των εξισώσεων και θεωρώντας στη θέση της την:
$x_{\Theta}+x_{K}+x_{\Xi}=1$ και λύνοντας το σύστημα, έχουμε:

$x_{\Theta}=\frac{8}{20}$ ή 40%
$x_{K}=\frac{9}{20}$ ή 45%
$x_{\Theta}=\frac{3}{20}$ ή 15%

Δηλαδή μακροπρόθεσμα ο πωλητής ο πωλητής επισκέπτεται τη Θεσσαλονίκη με πιθανότητα 40%, την Καβάλα με πιθανότητα 45% και την Ξάνθη με πιθανότητα 15%.

2 ΚΕΦΑΛΑΙΟ 2 ΚΡΥΠΤΟΓΡΑΦΙΑ

2.1 ΚΡΥΠΤΟΓΡΑΦΙΑ:

Σε αυτό το κεφάλαιο θα ασχοληθούμε με μια άλλη εφαρμογή της γραμμικής Άλγεβρας, την Κρυπτογραφία.
Κρυπτογραφία είναι η επιστήμη που ασχολείται με τη μελέτη, και την ανάπτυξη των τεχνικών κρυπτογράφησης κι αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχόμενου μηνυμάτων.
Η κρυπτογραφία αποτελεί επιστημονικό κλάδο μεγάλης σημασίας μιας και η συνεισφορά της κυρίως στους τομείς της ασφάλειας υπολογιστικών συστημάτων και επικοινωνιών είναι τεράστια.

2.2 ΙΣΤΟΡΙΚΗ ΑΝΑΦΟΡΑ

Ιστορικά η κρυπτογραφία χρησιμοποιήθηκε για το μετασχηματισμό μηνυμάτων από μια κανονική μορφή σε έναν ακατανόητο γρίφο, ώστε να αποφευχθεί η υποκλοπή του από τρίτους.
Η κρυπτογραφία χρησιμοποιείται ως τεχνική ήδη από την αρχαιότητα όπως στη Μεσοποταμία το 1500 π.Χ. και στη Αρχαία Σπάρτη τον $5^{ο}$ π.Χ. αιώνα με τις περίφημες σκυτάλες. Όλες αυτές οι προσπάθειες δείχνουν την ανάγκη που υπήρχε από τη αρχαιότητα κιόλας να παραμείνει ιδιωτική κάποια πληροφορία καθώς και τη ευρηματικότητα των δημιουργών των συστημάτων αυτών.

Κρυπτεία Σκυτάλη ένα από τα αρχαιότερα συστήματα κρυπτογράφησης.

Εικόνα 3 Κρύπτεια σκυτάλη

Κατά τη διάρκεια του 20^{ου} αιώνα κατασκευάστηκαν αρκετές μηχανικές συσκευές που έκαναν αυτόματη αντικατάσταση.
Η πιο διάσημη από αυτές ήταν η συσκευή *Enigma*, η οποία χρησιμοποιήθηκε από τους Γερμανούς κατά τη διάρκεια του Β' Παγκοσμίου Πολέμου για την αποστολή μυστικών μηνυμάτων στα στρατεύματα τους.
Ο κώδικας αναγνωρίστηκε από τους συμμάχους, αν και οι Γερμανοί άργησαν να αντιληφθούν ότι τα μυστικά τους αποκρυπτογραφούνταν.

Η μηχανή Enigma

Εικόνα 4 Μηχανή Enigma

Παρόλο που οι κρυφοί κώδικες φτάνουν στις αρχικές μέρες της γραπτής επικοινωνίας υπάρχει τελευταία μια έκρηξη ενδιαφέροντος για το θέμα λόγω της ανάγκης να διατηρηθεί η ιδιωτικότητα της πληροφορίας η οποία αναμεταδίδεται μέσα από δημόσιες γραμμές επικοινωνίας.

2.3 ΟΡΙΣΜΟΙ

Στη γλώσσα της κρυπτογραφίας , οι κώδικες καλούνται *κρυπτογραφήματα* (cipher) , το αρχικό, μη κρυπτογραφημένο κείμενο (*plaintext*) και το κρυπτογραφημένο κείμενο (*cipher text*).
Η διαδικασία μετατροπής του αρχικού κειμένου σε κρυπτογραφημένο καλείται *κρυπτογράφηση* και η αντίστροφη διαδικασία ,της μετατροπής ενός κρυπτογραφημένου κειμένου σε απλό καλείται *αποκρυπτογράφηση*..

2.4 ΚΡΥΠΤΟΓΡΑΦΗΜΑΤΑ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ

Τα απλούστερα κρυπτογραφήματα είναι τα κρυπτογραφήματα αντικατάστασης (substitution ciphers) και είναι αυτά τα οποία αντικαθιστούν κάθε γράμμα της αλφαβήτου με ένα διαφορετικό γράμμα.

Για παράδειγμα στο παρακάτω κρυπτογράφημα αντικατάστασης:

Αρχικό: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Κρυπτογραφημένο: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Το αρχικό γράμμα A αντικαθίσταται από το D το γράμμα B από το E και ούτω καθεξής.
ROME WAS NOT BUILT IN A DAY γίνεται
URPH ZPV QRW EXLOW LQP GDB

Το μειονέκτημα των κρυπτογραφημάτων αντικατάστασης είναι ότι διατηρούν τη συχνότητα των μεμονωμένων γραμμάτων κάνοντας σχετικά εύκολο το σπάσιμο του κώδικα με στατιστικές μεθόδους.
Ένας τρόπος για να ξεπεράσουμε αυτό το πρόβλημα είναι να χωρίσουμε το αρχικό κείμενο σε ομάδες γραμμάτων και να κρυπτογραφήσουμε το απλό κείμενο ανά ομάδα αντί για ένα γράμμα τη φορά.

2.5 ΠΟΛΥΓΡΑΦΙΚΟ ΣΥΣΤΗΜΑ

Το σύστημα της κρυπτογράφησης στο οποίο το αρχικό κείμενο χωρίζεται σε ομάδες γραμμάτων από ν γράμματα καθένα από τα οποία αντικαθίσταται από κρυπτογραφημένα γράμματα καλείται πολυγραφικό σύστημα.
Σε αυτό το τμήμα θα παρουσιάσουμε το πολυγραφικό σύστημα το οποίο βασίζεται σε μετασχηματισμούς πινάκων.

2.6 ΚΡΥΠΤΟΓΡΑΦΗΜΑ HILL

Το κρυπτογράφημα στο οποίο αναφερόμαστε ονομάζεται κρυπτογράφημα Hill από τον Lester S. Hill (1891-1961) ο οποίος το παρουσίασε σε δύο εργασίες, «Cryptography in an Algebraic Alphabet» American Mathematical Monthly 36 (June-July 1929) και « Concerning Certain Linear Transformation Apparatus of Cryptography» American Mathematical Monthly 38 (March 1931).
Παρακάτω υποθέτουμε ότι σε κάθε γράμμα στο αρχικό κείμενο και στο κρυπτογραφημένο εκτός από το Z αντιστοιχεί ένας αριθμός ο οποίος προσδιορίζει τη θέση του στο βασικό αλφάβητο.
Για λόγους για τους οποίους θα καταλάβουμε καλύτερα αργότερα , στο γράμμα Z αντιστοιχεί η τιμή 0.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Πίνακας 4 Πίνακας κρυπτογραφήματος Hill

Στο απλούστερο κρυπτογράφημα Hill διαδοχικά ζευγάρια γραμμάτων του αρχικού κειμένου μετασχηματίζονται σε κρυπτογραφημένο κείμενο με την ακόλουθη διαδικασία.
Βήμα 1: Διαλέγουμε έναν πίνακα 2×2 με ακέραιες καταχωρίσεις A = $\begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$ για να εκτελέσουμε την κρυπτογράφηση. Μερικές πρόσθετες συνθήκες στον A θα επιβληθούν αργότερα.
Βήμα 2: Ταξινομούμε διαδοχικά γράμματα του αρχικού κειμένου σε ζευγάρια, προσθέτοντας ένα αυθαίρετο γράμμα για να συμπληρωθεί το τελευταίο ζευγάρι εάν το αρχικό κείμενο έχει περιττό πλήθος γραμμάτων και αντικαθιστούμε κάθε γράμμα του αρχικού κειμένου με τον αριθμό του.
Βήμα 3: Διαδοχικά μετατρέπουμε κάθε ζευγάρι γραμμάτων του αρχικού κειμένου p_1 p_2 σε διάνυσμα στήλη
P = $\begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ και δημιουργούμε το αποτέλεσμα A·P.
Καλούμε P το διάνυσμα του αρχικού κειμένου και A·P το αντίστοιχο κρυπτογραφημένο διάνυσμα.
Βήμα 4 : Μετατρέπουμε κάθε κρυπτογραφημένο διάνυσμα στο αντίστοιχο αλφαβητικό.

Παράδειγμα 1:

Χρησιμοποιώντας τον πίνακα A = $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix}$ δημιουργούμε το κρυπτογράφημα Hill για το αρχικό μήνυμα

I AM HIDING

Ταξινομούμε διαδοχικά τα γράμματα σε ζευγάρια προσθέτοντας το αυθαίρετο γράμμα G για να συμπληρώσουμε το τελευταίο ζευγάρι

IA M H ID IN GG

ή αντίστοιχα από τον πίνακα

9 1 13 8 9 4 9 14 7 7

Για να κρυπτογραφήσουμε το ζευγάρι IA δημιουργούμε το αποτέλεσμα

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} \cdot \begin{bmatrix}9\\1\end{bmatrix} = \begin{bmatrix}11\\3\end{bmatrix}$$

το οποίο από τον πίνακα βλέπουμε ότι αντιστοιχεί στα γράμματα KC.
Για να κρυπτογραφήσουμε το ζευγάρι MH δημιουργούμε το αποτέλεσμα

$$\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} \cdot \begin{bmatrix}13\\18\end{bmatrix} = \begin{bmatrix}29\\24\end{bmatrix} \qquad (1)$$

Όμως εδώ παρατηρούμε ένα πρόβλημα , ο αριθμός 29 δεν αντιστοιχεί σε κανένα γράμμα στον πίνακα. Για την επίλυση αυτού του προβλήματος κάνουμε την παρακάτω συμφωνία :

Όταν εμφανίζεται ένας ακέραιος μεγαλύτερος του 25 θα αντικαθίσταται από το υπόλοιπο της Ευκλείδειας διαίρεσης του ακέραιου αυτού με το 26.

Επειδή το υπόλοιπο της διαίρεσης με το 26 είναι ένας από τους ακέραιους 0,1,2,3,…,25 αυτή η διαδικασία θα αποδίδει πάντα έναν ακέραιο με αλφαβητικό ισοδύναμο από τον πίνακα.
Έτσι, αντικαθιστούμε στην (1) το 29 με το 3 το οποίο είναι το υπόλοιπο της διαίρεσης 29 δια 26. Από τον πίνακα βλέπουμε ότι τα γράμματα στα οποία αντιστοιχεί είναι CX. Άρα το κρυπτογραφημένο κείμενο για το ζευγάρι MH είναι το ζευγάρι CX.

Το επόμενο ζευγάρι ID έχει διάνυσμα στήλη $\begin{bmatrix}9\\4\end{bmatrix}$ και για το κρυπτογραφημένο

δημιουργούμε το γινόμενο $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} \cdot \begin{bmatrix}9\\4\end{bmatrix} = \begin{bmatrix}17\\12\end{bmatrix}$ άρα αντιστοιχεί στα γράμματα QL.

Συνεχίζουμε στο επόμενο $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} \cdot \begin{bmatrix}9\\14\end{bmatrix} = \begin{bmatrix}37\\42\end{bmatrix}$ ή $\begin{bmatrix}11\\16\end{bmatrix}$ το οποίο αντιστοιχεί στα γράμματα KP.

Για το τελευταίο ζευγάρι GG $\begin{bmatrix}7\\7\end{bmatrix}$ έχουμε $\begin{bmatrix}1 & 2\\0 & 3\end{bmatrix} \cdot \begin{bmatrix}7\\7\end{bmatrix} = \begin{bmatrix}21\\21\end{bmatrix}$ και τα αντίστοιχα γράμματα είναι UU.

Άρα τα κρυπτογραφημένα γράμματα μας είναι KH CX QL KP UU τα οποία συνήθως μεταδίδονται σε σειρά χωρίς κενά ανάμεσα τους.

KHCXQLKPUU

Επειδή το αρχικό κείμενο είχε ομαδοποιηθεί σε ζευγάρια και κρυπτογραφήθηκε με έναν πίνακα 2×2 στο παράδειγμα 1 το συγκεκριμένο κρυπτογράφημα Hill αναφέρεται ως **Hill 2-cipher.**

Προφανώς είναι δυνατόν να ομαδοποιήσουμε το αρχικό κείμενο σε ομάδες των τριών γραμμάτων και να χρησιμοποιήσουμε πίνακα 3×3 με ακέραιες εγγραφές, αυτό καλείται **Hill 3-cipher.**

Γενικά, για ένα **Hill n-cipher,** το αρχικό κείμενο ομαδοποιείται σε ομάδες n γραμμάτων και χρησιμοποιείται για την κρυπτογράφηση ένας n×n πίνακας με ακέραιες εγγραφές.

2.7 Modular Arithmetic –Αριθμητική Υπολοίπων

Στο παράδειγμα 1 , οι ακέραιοι μεγαλύτεροι του 26 αντικαθίστανται από τα υπόλοιπά τους μετά την διαίρεση με το 26. Αυτή η τεχνική κατά την οποία δουλεύουμε με τα υπόλοιπα ονομάζεται Αριθμητική Υπολοίπων. Λόγω της σπουδαιότητας της στην κρυπτογραφία θα ασχοληθούμε λίγο με αυτήν την Αριθμητική.
Στην Αριθμητική των υπολοίπων έχουμε έναν ακέραιο m ο οποίος καλείται modulus και όποιοι δύο ακέραιοι των οποίων η διαφορά είναι πολλαπλάσιο του m λέμε ότι είναι ισοδύναμοι modulo m.

2.7.1 **Ορισμός**

Εάν m είναι ένας θετικός ακέραιος και a, b είναι οποιοιδήποτε ακέραιοι τότε λέμε ότι ο a είναι ισοδύναμος με τον b modulo m και γράφουμε ***a=b (mod m)*** εάν αφήνουν το ίδιο υπόλοιπο όταν διαιρούνται με τον m δηλαδή η διαφορά a – b είναι ένας ακέραιος πολλαπλάσιο του m.

Παράδειγμα 2:

Διάφορες ισοδυναμίες:
7 = 2 (mod5)
-1 = 25 (mod26)
12 = 0 (mod4)

Για κάθε modulus m μπορεί να αποδειχθεί ότι κάθε ακέραιος a είναι ισοδύναμος ακριβώς με έναν από τους ακέραιους 0,1,2,…,m-1.
Επομένως για κάθε θετικό ακέραιο m το σύνολο των ακεραίων κατανέμεται σε m κλάσεις ισοδυναμίας σε σχέση με τα υπόλοιπά τους , τις κλάσεις 0,1,2,…, m-1.
Κάθε κλάση αντιστοιχεί σε ένα από τα m πιθανά υπόλοιπα 0.1.2…..m-1 της διαίρεσης ενός ακεραίου με το m. Το σύνολο των διαφορετικών κλάσεων modm δηλώνεται ως Z_m = $\{0,1,2,\dots,m-1\}$

2.7.2 **Θεώρημα :**

Για κάθε ακέραιο a και modulus m ορίζουμε R= υπόλοιπο της διαίρεσης $\frac{|a|}{m}$ τότε το υπόλοιπο r δίνεται από r = $\begin{cases} R \quad \text{εάν } a \geq 0 \\ m - R \text{ εάν } \alpha < 0 \text{ και } R \neq 0 \\ 0 \text{ εάν } a < 0 \text{ και } R = 0 \end{cases}$

Παράδειγμα 3:

Υπόλοιπο r mod26

Θέλουμε να βρούμε το υπόλοιπο r mod26 των αριθμών
Α) 87, Β) -38, Γ) -26

Α) διαιρούμε $|87| = 87$ με το 26 και έχουμε $87=26\cdot 3 + 9$ άρα R = 9 και σύμφωνα με το θεώρημα παραπάνω r = 9 έτσι

$$87=9 \pmod{26}$$

Β) διαιρούμε $|-38| = 38$ με το 26 και έχουμε $38=26\cdot 1 + 12$ άρα R = 12 και σύμφωνα με το θεώρημα παραπάνω r = m-R=26-12=14 έτσι

$$-38=14 \pmod{26}$$

Γ) διαιρούμε $|-26| = 26$ με το 26 και έχουμε $26=26\cdot 1 + 0$ άρα R = 0 και σύμφωνα με το θεώρημα παραπάνω r = 0 έτσι

$$-26=0 \pmod{26}$$

2.8 ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ

2.8.1 **Ορισμός**

Αντίστροφος:

Όπως γνωρίζουμε κάθε μη μηδενικός αριθμός α έχει έναν αντίστροφο ο οποίος συμβολίζεται α^{-1} και ισχύει

$$\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$$

Στην αριθμητική των υπολοίπων έχουμε την παρακάτω έννοια

2.8.2 **Ορισμός**

Εάν α είναι ένας αριθμός στο Z_m τότε ο αριθμός α^{-1} στο Z_m καλείται αντίστροφος του α modulo m εάν $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$ (modm).
Αποδεικνύεται ότι εάν ο α και ο m δεν έχουν κοινούς πρώτους παράγοντες , τότε ο α έχει μοναδικό αντίστροφο modulo m. Αντίθετα εάν ο α και ο m έχουν κοινούς πρώτους παράγοντες , τότε ο α δεν έχει αντίστροφο modulo m.

Παράδειγμα 4: Ο αντίστροφος του 3 modulo 26

Ο αριθμός 3 έχει αντίστροφο modulo 26 γιατί οι αριθμοί 3 και 26 είναι πρώτοι μεταξύ τους, δεν έχουν κοινούς πρώτους παράγοντες.
Αυτός ο αντίστροφος μπορεί να βρεθεί λύνοντας την παρακάτω εξίσωση:

$$3 \cdot x = 1 \pmod{26}$$

Παρόλο που υπάρχουν γενικές μέθοδοι επίλυσης αυτών των εξισώσεων δεν θα ασχοληθούμε με αυτές. Επειδή ο αριθμός 26 είναι σχετικά μικρός θα δοκιμάσουμε τους αριθμούς από το Z_m ποιος ικανοποιεί την εξίσωση, με αυτή την προσέγγιση βρίσκουμε x=9 διότι

$$3 \cdot 9 = 27 = 1 \pmod{26}$$
$$\text{Άρα } 3^{-1} = 9 \pmod{26}$$

Παράδειγμα 5 : Ένας αριθμός που δεν έχει αντίστροφο Modulo 26
Ο αριθμός 4 δεν έχει αντίστροφο modulo 26 γιατί οι αριθμοί 4 και 26 έχουν κοινό πρώτο παράγοντα τον αριθμό 2.

Για μελλοντική αναφορά στον πίνακα 2 έχουμε τους αντίστροφους modulo 26

α	1	3	5	7	9	11	15	17	19	21	23	25
α^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

Πίνακας 5 Αντίστροφοι modulo26

Για να είναι χρήσιμος ένας κώδικας κρυπτογράφησης πρέπει να έχει και μια εύχρηστη διαδικασία αποκρυπτογράφησης . Στην περίπτωση που μελετάμε, του κώδικα Hill η αποκρυπτογράφηση χρησιμοποιεί τον αντίστροφο modulo 26 από τον πίνακα κρυπτογράφησης .
Για να είμαστε ακριβείς , εάν m είναι ένας θετικός ακέραιος , τότε ο τετραγωνικός πίνακας A με εγγραφές στο Z_m λέγεται αντιστρέψιμος modulo m εάν υπάρχει πίνακας B με εγγραφές στο Z_m τέτοιος ώστε

$$A \cdot B = B \cdot A = I \ (\mathrm{mod} m)$$

Έστω ότι ο $A = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$ είναι ένας αντιστρέψιμος modulo 26 πίνακας και αυτός χρησιμοποιείται σε έναν Hill-2 κώδικα κρυπτογραφήματος.

Εάν $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ είναι ένα αρχικό διάνυσμα τότε $c = A \cdot P \ (\mathrm{mod}26)$ είναι το αντίστοιχα κρυπτογραφημένο διάνυσμα και $P = A^{-1} \cdot c \ (\mathrm{mod}26)$.

Έτσι καταλαβαίνουμε ότι κάθε αρχικό διάνυσμα μπορεί να ανακτηθεί από το αντίστοιχο κρυπτογραφημένο διάνυσμα πολλαπλασιάζοντας το από αριστερά με τον πίνακα A^{-1} (mod26).
Οπότε καταλαβαίνουμε ότι στην κρυπτογραφία είναι πολύ σημαντικό να γνωρίζουμε ποιοι πίνακες είναι αντιστρέψιμοι modulo 26 και πως βρίσκουμε τους αντίστροφους.
Όπως γνωρίζουμε από την Άλγεβρα ένας τετραγωνικό πίνακας είναι αντιστρέψιμος αν και μόνο αν η ορίζουσα του det(A) ≠0 ή ισοδύναμα αν η det(A) έχει αντίστροφο.
Το παρακάτω Θεώρημα είναι ανάλογο των παραπάνω στην Αριθμητική των Υπολοίπων,

2.8.3 **Θεώρημα :**

Ένας τετραγωνικός πίνακας A με εγγραφές στο Z_m είναι αντιστρέψιμος modulo m αν και μόνο αν το υπόλοιπο r της ορίζουσας det(A) modulo m έχει αντίστροφο modulo m. Επειδή το υπόλοιπο r της ορίζουσας det(A) modulo m θα έχει αντίστροφο modulo m αν και μόνο αν αυτό το υπόλοιπο και ο m δεν έχουν κοινούς πρώτους παράγοντες έχουμε το παρακάτω πόρισμα.

2.8.4 **Πόρισμα :**

Ένας τετραγωνικός πίνακας A με εγγραφές στο Z_m είναι αντιστρέψιμος modulo m αν και μόνο αν το υπόλοιπο r της ορίζουσας det(A) modulo m και ο m δεν έχουν κοινούς πρώτους παράγοντες.
Επειδή οι μόνοι πρώτοι παράγοντες του m=26 είναι ο 2 και ο 13 έχουμε το παρακάτω συμπέρασμα , πολύ χρήσιμο στην κρυπτογραφία.

2.8.5 **Πόρισμα :**

Ένας τετραγωνικός πίνακας A με εγγραφές στο Z_{26} είναι αντιστρέψιμος modulo 26 αν και μόνο αν το υπόλοιπο r της ορίζουσας det(A) δεν διαιρείται με το 2 ή το 13.

Σύμφωνα με τα παραπάνω έχουμε A = $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ έχει εγγραφές στο Z_{26} και το υπόλοιπο r της det(A) = ad-bc modulo 26 δεν διαιρείται με το 2 ή το 13 τότε ο αντίστροφος του A (mod26) δίνεται από τον τύπο:

$$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \text{(mod26)} \qquad (2)$$

Όπου $(ad - bc)^{-1}$ είναι ο αντίστροφος του υπολοίπου (ad-bc) (mod26).

Παράδειγμα 6 Αντίστροφος πίνακα modulo 26

Ας βρούμε τον αντίστροφο του πίνακα $A = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix}$ Modulo 26

Βρίσκουμε την ορίζουσα det(A) = αd-bc = 5·3-2·6 = 15-12 = 3
Από τον πίνακα 2 βρίσκουμε τον αντίστροφο modulo 26
$(ad - bc)^{-1} = 3^{-1} = 9$ (mod26)

Έτσι από τη σχέση (2) έχουμε

$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ (mod26) $= 3^{-1} \cdot \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = 9 \cdot \begin{bmatrix} 3 & -6 \\ -2 & 5 \end{bmatrix} = \begin{bmatrix} 27 & -54 \\ -12 & 45 \end{bmatrix} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix}$ (mod26).

Ας το επαληθεύσουμε $A \cdot A^{-1} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} = \begin{bmatrix} 53 & 234 \\ 26 & 105 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (mod26)

$A^{-1} \cdot A = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} = \begin{bmatrix} 53 & 78 \\ 78 & 105 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (mod26)

Παράδειγμα 7: Αποκρυπτογράφηση ενός Hill-2 κώδικα κρυπτογράφησης

Ας αποκρυπτογραφήσουμε το Hill-2 κρυπτογραφημένο μήνυμα το οποίο κρυπτογραφήσαμε με τον πίνακα του παραδείγματος 6.

GTNKGKDUSK

Από τον πίνακα 1 τα αριθμητικά αντίστοιχα από αυτό το κρυπτογραφημένο κείμενο είναι τα 7 20 14 11 7 11 4 21 19 11

Για ανακτήσουμε τα αρχικά ζευγάρια πολλαπλασιάζουμε κάθε κρυπτογραφημένο διάνυσμα με τον αντίστροφο του Α που έχουμε από το παράδειγμα 6.

$$p = A^{-1} \cdot c = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 487 \\ 436 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 11 \end{bmatrix} = \begin{bmatrix} 278 \\ 321 \end{bmatrix} = \begin{bmatrix} 18 \\ 9 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 11 \end{bmatrix} = \begin{bmatrix} 271 \\ 265 \end{bmatrix} = \begin{bmatrix} 11 \\ 5 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 21 \end{bmatrix} = \begin{bmatrix} 508 \\ 431 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} \pmod{26}$$

$$\begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 19 \\ 11 \end{bmatrix} = \begin{bmatrix} 283 \\ 361 \end{bmatrix} = \begin{bmatrix} 23 \\ 23 \end{bmatrix} \pmod{26}$$

Από τον πίνακα 1 και τα αλφαβητικά ισοδύναμα έχουμε:

ST RI KE NO WW

Το οποίο αντιστοιχεί στο μήνυμα

STRIKE NOW

2.9 ΚΡΥΠΤΑΝΑΛΥΣΗ

Κρυπτανάλυση ονομάζεται η μελέτη τρόπων αποκωδικοποίησης υποκλαπέντων μηνυμάτων για τα οποία δεν είναι γνωστό το κλειδί ,δηλαδή το σπάσιμο του κώδικα.
Με τον όρο *κλειδί* δηλώνεται η συγκεκριμένη πληροφορία σχετικά με την κωδικοποίηση του μηνύματος, δηλαδή το πώς γίνεται η αποκωδικοποίησή του.
Επειδή ο σκοπός των κρυπτογραφημένων μηνυμάτων και πληροφοριών είναι να εμποδίσει τους αντίπαλους να μάθουν το περιεχόμενο τους, οι κρυπτογράφοι ανησυχούν για την ασφάλεια των κωδικών τους. Δηλαδή πόσο εύκολα ο αντίπαλος μπορεί να σπάσει τον κώδικα. Εδώ θα δούμε μια τεχνική σπασίματος του κώδικα Hill.
Ας υποθέσουμε ότι καταφέραμε να αποκτήσουμε κάποιο αρχικό μήνυμα και το αντίστοιχο κρυπτογραφημένο.
Για παράδειγμα εξετάζοντας κάποιο μήνυμα που έχουμε υποκλέψει, μπορούμε να συμπεράνουμε ότι το μήνυμα είναι ένα γράμμα , το οποίο ξεκινάει DEAR SIR.
Θα δούμε ότι μόνο με αυτά τα λίγα δεδομένα θα καταφέρουμε να αποκωδικοποιήσουμε τον κώδικα Hill και έτσι να έχουμε πρόσβαση και στο υπόλοιπο κρυπτογραφημένο μήνυμα.
Είναι στοιχειώδες συμπέρασμα στη Γραμμική Άλγεβρα , ότι ένας γραμμικός μετασχηματισμός είναι ολοκληρωτικά καθορισμένος από τις τιμές της βάσης.
Αυτή η αρχή υποδεικνύει εάν έχουμε έναν Hill n-cipher και εάν

$$p_1, p_2, p_3, \ldots, p_n$$

είναι γραμμικώς ανεξάρτητα διανύσματα που αντιστοιχούν στο μη κρυπτογραφημένο μήνυμα και των οποίων τα κρυπτογραφημένα διανύσματα είναι

$$Ap_1, Ap_2, Ap_3, \ldots, Ap_n$$

είναι γνωστά, τότε υπάρχουν αρκετές πληροφορίες ικανές για να προσδιορίσουμε τον πίνακα A και επομένως τον A^{-1} (modm).

2.9.1 **Θεώρημα : Καθορισμός του πίνακα αποκρυπτογράφησης.**

Έστω $p_1, p_2, p_3, \ldots, p_n$ είναι τα γραμμικώς ανεξάρτητα διανύσματα που αντιστοιχούν στο μη κρυπτογραφημένο μήνυμα και $c_1, c_2, c_3, \ldots, c_n$ τα αντίστοιχα κρυπτογραφημένα διανύσματα με κώδικα Hill.

Εάν $P=\begin{bmatrix} p_1^T \\ p_2^T \\ \ldots \\ p_n^T \end{bmatrix}$

Είναι ο n×n πίνακας με γραμμές τα διανύσματα $p_1^T, p_2^T, \ldots, p_n^T$ και εάν

$$C=\begin{bmatrix} c_1^T \\ c_2^T \\ \ldots \\ c_n^T \end{bmatrix}$$

Είναι ο n×n πίνακας με γραμμές τα διανύσματα $c_1^T, c_2^T, \ldots, c_n^T$, τότε η ακολουθία των στοιχειωδών εργασιών που απλοποιεί τον C στον I , μετατρέπει τον P στον $(A^{-1})^T$.
Αυτό το Θεώρημα μας λέει ότι για να βρούμε τον πίνακα αποκωδικοποίησης A^{-1}, πρέπει να βρούμε την ακολουθία των διεργασιών που απλοποιούν τον C στον I και μετά να ακολουθήσουμε την ίδια ακολουθία από διεργασίες στον P.

Παράδειγμα 8:
Έχει υποκλαπεί το παρακάτω, κωδικοποιημένο με Hill-2 κώδικα, μήνυμα.

IOSBTGXESPXHOPDE

Ας αποκρυπτογραφήσουμε το μήνυμα ξέροντας ότι αρχίζει με τη λέξη DEAR.

Από τον πίνακα 1 τα αριθμητικά ισοδύναμα του αρχικού κειμένου είναι:

D E	A R
4 5	1 18

Και τα αριθμητικά ισοδύναμα του αντίστοιχου κρυπτογραφημένου κειμένου είναι

I O	S B
9 15	19 2

Έτσι τα αντίστοιχα αρχικά και κρυπτογραφημένα διανύσματα είναι:

$$p_1 = \begin{bmatrix} 4 \\ 5 \end{bmatrix} \leftrightarrow c_1 = \begin{bmatrix} 9 \\ 15 \end{bmatrix}$$

$$p_2 = \begin{bmatrix} 1 \\ 18 \end{bmatrix} \leftrightarrow c_2 = \begin{bmatrix} 19 \\ 2 \end{bmatrix}$$

έτσι έχουμε

$$C = \begin{bmatrix} {c_1}^T \\ {c_2}^T \end{bmatrix} = \begin{bmatrix} 9 & 15 \\ 19 & 2 \end{bmatrix}$$

Τον οποίο θέλουμε να τον απλοποιήσουμε στον I με στοιχειώδεις διεργασίες και μετά να εφαρμόσουμε τις ίδιες ακριβώς στον

$$P = \begin{bmatrix} {p_1}^T \\ {p_2}^T \end{bmatrix} = \begin{bmatrix} 4 & 5 \\ 1 & 18 \end{bmatrix}$$

για να βρούμε τον $(A^{-1})^T$.

Αυτό μπορεί να επιτευχθεί εάν συνδέσουμε τον P δεξιά του C και εφαρμόζουμε τις διεργασίες στον πίνακα [C ׀ P] μέχρι το αριστερό μέλος να απλοποιηθεί στον I.
Έτσι ο τελικός πίνακας θα έχει τη μορφή [I ׀ $(A^{-1})^T$P].

Τους υπολογισμούς τους βλέπουμε παρακάτω:

$\left(\begin{array}{cc|cc} 9 & 15 & 4 & 5 \\ 19 & 2 & 1 & 18 \end{array}\right)$ ← Σχηματίζουμε τον πίνακα [C ׀ P]

$\left(\begin{array}{cc|cc} 27 & 45 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right)$ ← Πολλαπλασιάζουμε την πρώτη γραμμή με το $9^{-1} = 3$

$\left(\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 19 & 2 & 1 & 18 \end{array}\right)$ ← Αντικαθιστούμε τους μεγαλύτερους από το 26 αριθμούς με το υπόλοιπό τους modulo 26, δηλαδή τον 27 με το 1 και τον 45 με το 19.

$\left(\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & -359 & -227 & -267 \end{array}\right)$ ← Πολλαπλασιάζουμε την πρώτη γραμμή με το -19 και την προσθέτουμε στη δεύτερη.

$\left(\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 5 & 7 & 19 \end{array}\right)$ ← Αντικαθιστούμε τους μεγαλύτερους από το 26 αριθμούς και τους αρνητικούς με το υπόλοιπό τους modulo 26, δηλαδή τον -359 με το 5, τον -227 με τον 7 και τον -267 με τον 19.

$\left(\begin{array}{cc|cc} 9 & 19 & 12 & 15 \\ 0 & 1 & 147 & 399 \end{array}\right)$ ← Πολλαπλασιάζουμε τη δεύτερη γραμμή με το $5^{-1} = 21$

$\left(\begin{array}{cc|cc} 1 & 19 & 12 & 15 \\ 0 & 1 & 17 & 9 \end{array}\right)$ ← Αντικαθιστούμε τους μεγαλύτερους από το 26 αριθμούς με το υπόλοιπό τους modulo 26, δηλαδή τον 147 με το 17 και τον 378 με τον 14.

$\left(\begin{array}{cc|cc} 1 & 0 & -311 & -156 \\ 0 & 1 & 17 & 9 \end{array}\right)$ ← Πολλαπλασιάζουμε τη δεύτερη γραμμή με το -19 και την προσθέτουμε στην πρώτη.

$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 17 & 9 \end{array}\right)$ ← Αντικαθιστούμε τους μεγαλύτερους από το 26 αριθμούς και τους αρνητικούς με το υπόλοιπό τους modulo 26, δηλαδή τον 147 με το 17 και τον 378 με τον 14.

Έτσι βρίσκουμε ότι

$$(A^{-1})^T = \begin{bmatrix} 1 & 0 \\ 17 & 9 \end{bmatrix}$$

Άρα ο πίνακας αποκρυπτογράφησης είναι:

$$A^{-1} = \begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix}$$

Για την αποκρυπτογράφηση ολόκληρου του μηνύματος , χωρίζουμε το μήνυμα σε ζευγάρια γραμμάτων και βρίσκουμε από τον πίνακα 1 τα αριθμητικά ισοδύναμα των γραμμάτων.

I O	S B	T G	X E	S P	X H	O P	D E
9 15	19 2	20 7	24 5	19 16	24 8	15 16	4 5

Μετά, πολλαπλασιάζουμε διαδοχικά τα κωδικοποιημένα διανύσματα που βρήκαμε παραπάνω με τον A^{-1} από αριστερά,

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 15 \end{bmatrix} = \begin{bmatrix} 264 \\ 135 \end{bmatrix} = \begin{bmatrix} 4 \\ 5 \end{bmatrix} (\text{mod}26) \begin{matrix} D \\ E \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 2 \end{bmatrix} = \begin{bmatrix} 53 \\ 18 \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \end{bmatrix} (\text{mod}26) \begin{matrix} A \\ R \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 20 \\ 7 \end{bmatrix} = \begin{bmatrix} 139 \\ 63 \end{bmatrix} = \begin{bmatrix} 9 \\ 11 \end{bmatrix} (\text{mod}26) \begin{matrix} I \\ K \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 5 \end{bmatrix} = \begin{bmatrix} 109 \\ 45 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} (\text{mod}26) \begin{matrix} E \\ S \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 19 \\ 16 \end{bmatrix} = \begin{bmatrix} 291 \\ 144 \end{bmatrix} = \begin{bmatrix} 5 \\ 14 \end{bmatrix} (\text{mod}26) \begin{matrix} E \\ N \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 24 \\ 8 \end{bmatrix} = \begin{bmatrix} 160 \\ 72 \end{bmatrix} = \begin{bmatrix} 4 \\ 20 \end{bmatrix} (\text{mod}26) \begin{matrix} D \\ T \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 287 \\ 144 \end{bmatrix} = \begin{bmatrix} 1 \\ 14 \end{bmatrix} (\text{mod}26) \begin{matrix} A \\ N \end{matrix}$$

$$\begin{bmatrix} 1 & 17 \\ 0 & 9 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \end{bmatrix} = \begin{bmatrix} 89 \\ 45 \end{bmatrix} = \begin{bmatrix} 11 \\ 19 \end{bmatrix} (\text{mod}26) \begin{matrix} K \\ S \end{matrix}$$

Τελικά ανακτούμε το μήνυμα από τα αρχικά ζευγάρια:

D E A R I K E S E N D T A N K S

DEAR IKE SEND TANKS

2.10 ΕΦΑΡΜΟΓΕΣ

2.10.1 **Εφαρμογή :**

Ας κωδικοποιήσουμε το παρακάτω μήνυμα

DARK NIGHT

με πίνακα κωδικοποίησης τον $A = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix}$

Πρώτα ελέγχουμε εάν ο πίνακας Α είναι αντιστρέψιμος modulo 26.

Βρίσκουμε την ορίζουσα det(A) = αd-bc = 4·2-3·1 = 8-3 = 5

Το 5 δεν διαιρεί το 26 άρα ο πίνακας μας αντιστρέφεται.

Από τον πίνακα 2 βρίσκουμε τον αντίστροφο modulo 26

$(ad - bc)^{-1} = 5^{-1} = 21 \pmod{26}$

Έτσι από τη σχέση (2) έχουμε

$A^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{26} = 5^{-1} \cdot \begin{bmatrix} 2 & -1 \\ -3 & 4 \end{bmatrix} = 21 \cdot \begin{bmatrix} 2 & -3 \\ -1 & 4 \end{bmatrix} = \begin{bmatrix} 42 & -21 \\ -63 & 84 \end{bmatrix} = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \pmod{26}.$

Ας το επαληθεύσουμε $A \cdot A^{-1} = \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} = \begin{bmatrix} 79 & 26 \\ 78 & 27 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}$

$A^{-1} \cdot A = \begin{bmatrix} 16 & 5 \\ 15 & 6 \end{bmatrix} \cdot \begin{bmatrix} 4 & 1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 79 & 26 \\ 78 & 27 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{26}.$

Άρα ο πίνακας Α είναι κατάλληλος για κωδικοποίηση.

Κωδικοποιούμε το μήνυμα

DARK NIGHT

Ταξινομούμε διαδοχικά τα γράμματα σε ζευγάρια προσθέτοντας το αυθαίρετο γράμμα G για να συμπληρώσουμε το τελευταίο ζευγάρι

DA RK NI GH TG

ή αντίστοιχα από τον πίνακα 4

4 1 18 11 14 9 7 8 20 7

Για να κρυπτογραφήσουμε το κάθε ζευγάρι δημιουργούμε το αποτέλεσμα c=Ap

$$\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix}\cdot\begin{bmatrix}4\\ 1\end{bmatrix}=\begin{bmatrix}17\\ 14\end{bmatrix}=\begin{bmatrix}17\\ 14\end{bmatrix}\ (\text{mod}26)\ \begin{matrix}Q\\ N\end{matrix}$$

$$\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix}\cdot\begin{bmatrix}18\\ 11\end{bmatrix}=\begin{bmatrix}83\\ 76\end{bmatrix}=\begin{bmatrix}5\\ 24\end{bmatrix}\ (\text{mod}26)\ \begin{matrix}E\\ X\end{matrix}$$

$$\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix}\cdot\begin{bmatrix}14\\ 9\end{bmatrix}=\begin{bmatrix}65\\ 60\end{bmatrix}=\begin{bmatrix}13\\ 8\end{bmatrix}\ (\text{mod}26)\ \begin{matrix}M\\ H\end{matrix}$$

$$\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix}\cdot\begin{bmatrix}7\\ 8\end{bmatrix}=\begin{bmatrix}36\\ 37\end{bmatrix}=\begin{bmatrix}10\\ 11\end{bmatrix}\ (\text{mod}26)\ \begin{matrix}J\\ K\end{matrix}$$

$$\begin{bmatrix}4 & 1\\ 3 & 2\end{bmatrix}\cdot\begin{bmatrix}20\\ 7\end{bmatrix}=\begin{bmatrix}87\\ 74\end{bmatrix}=\begin{bmatrix}9\\ 22\end{bmatrix}\ (\text{mod}26)\ \begin{matrix}I\\ V\end{matrix}$$

Άρα το κωδικοποιημένο μήνυμα μας είναι

QNEXMHJKIV

2.10.2 **Εφαρμογή :**

Ας αποκωδικοποιήσουμε το παραπάνω μήνυμα.

QN EX MH JK IV

Από τον πίνακα 4 τα αριθμητικά αντίστοιχα από αυτό το κρυπτογραφημένο κείμενο είναι τα

17 14 5 24 13 8 10 11 9 22

Για ανακτήσουμε τα αρχικά ζευγάρια πολλαπλασιάζουμε κάθε κρυπτογραφημένο διάνυσμα με τον αντίστροφο του A που έχουμε από την εφαρμογή 3.10.1.

p= A^{-1} ·c =

$$\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\cdot\begin{bmatrix}17\\14\end{bmatrix}=\begin{bmatrix}342\\339\end{bmatrix}=\begin{bmatrix}4\\1\end{bmatrix}\ (\text{mod}26)\quad \begin{matrix}D\\A\end{matrix}$$

$$\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\cdot\begin{bmatrix}5\\24\end{bmatrix}=\begin{bmatrix}200\\219\end{bmatrix}=\begin{bmatrix}18\\11\end{bmatrix}\ (\text{mod}26)\quad \begin{matrix}R\\K\end{matrix}$$

$$\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\cdot\begin{bmatrix}13\\8\end{bmatrix}=\begin{bmatrix}248\\243\end{bmatrix}=\begin{bmatrix}14\\9\end{bmatrix}\ (\text{mod}26)\quad \begin{matrix}N\\I\end{matrix}$$

$$\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\cdot\begin{bmatrix}10\\11\end{bmatrix}=\begin{bmatrix}215\\216\end{bmatrix}=\begin{bmatrix}7\\8\end{bmatrix}\ (\text{mod}26)\quad \begin{matrix}G\\H\end{matrix}$$

$$\begin{bmatrix}16 & 5\\ 15 & 6\end{bmatrix}\cdot\begin{bmatrix}9\\22\end{bmatrix}=\begin{bmatrix}254\\267\end{bmatrix}=\begin{bmatrix}20\\7\end{bmatrix}\ (\text{mod}26)\quad \begin{matrix}T\\G\end{matrix}$$

Από τον πίνακα 4 και τα αλφαβητικά ισοδύναμα έχουμε:

DARKNIGHTG

DARK NIGHT

2.10.3 **Εφαρμογή :**

Ας αποκωδικοποιήσουμε το παρακάτω μήνυμα το οποίο είναι κωδικοποιημένο με τον κώδικα Hill-2

LNGIHGYBVRENJYQO

Εάν ξέρουμε ότι τα τέσσερα τελευταία γράμματα είναι ATOM.

Ας αποκρυπτογραφήσουμε το μήνυμα ξέροντας ότι τα τέσσερα τελευταία γράμματα είναι ATOM .

Από τον πίνακα 4 τα αριθμητικά ισοδύναμα του αρχικού κειμένου είναι:

A	T	O	M
1	20	15	13

Και τα αριθμητικά ισοδύναμα του αντίστοιχου κρυπτογραφημένου κειμένου είναι

J	Y	Q	O
10	25	17	15

Έτσι τα αντίστοιχα αρχικά και κρυπτογραφημένα διανύσματα είναι:

$$p_1 = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \leftrightarrow c_1 = \begin{bmatrix} 10 \\ 25 \end{bmatrix}$$
$$p_2 = \begin{bmatrix} 15 \\ 13 \end{bmatrix} \leftrightarrow c_2 = \begin{bmatrix} 17 \\ 15 \end{bmatrix}$$

έτσι έχουμε

$$C = \begin{bmatrix} {c_1}^T \\ {c_2}^T \end{bmatrix} = \begin{bmatrix} 10 & 25 \\ 17 & 15 \end{bmatrix}$$

Τον οποίο θέλουμε να τον απλοποιήσουμε στον I με στοιχειώδεις διεργασίες και μετά να εφαρμόσουμε τις ίδιες ακριβώς στον

$$P = \begin{bmatrix} {p_1}^T \\ {p_2}^T \end{bmatrix} = \begin{bmatrix} 1 & 20 \\ 15 & 13 \end{bmatrix}$$

για να βρούμε τον $(A^{-1})^T$.

$\left(\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 17 & 15 & 15 & 13 \end{array}\right)$ ← Σχηματίζουμε τον πίνακα [C I P]

$\left(\begin{array}{cc|cc} 10 & 25 & 1 & 20 \\ 119 & 105 & 105 & 91 \end{array}\right)$ ← Πολλαπλασιάζουμε την δεύτερη γραμμή με το $15^{-1} = 7$

$\left(\begin{matrix}10 & 25\\ 15 & 1\end{matrix}\middle|\begin{matrix}1 & 20\\ 1 & 13\end{matrix}\right)$ ← Αντικαθιστούμε τους αριθμούς με το υπόλοιπό τους modulo 26.

$\left(\begin{matrix}-365 & 0\\ 15 & 1\end{matrix}\middle|\begin{matrix}-24 & -305\\ 1 & 13\end{matrix}\right)$ ← Πολλαπλασιάζουμε την δεύτερη γραμμή με το -25 και την προσθέτουμε στην πρώτη.

$\left(\begin{matrix}25 & 0\\ 15 & 1\end{matrix}\middle|\begin{matrix}2 & 7\\ 1 & 13\end{matrix}\right)$ ← Αντικαθιστούμε τους αριθμούς με το υπόλοιπό τους modulo 26.

$\left(\begin{matrix}625 & 0\\ 15 & 1\end{matrix}\middle|\begin{matrix}50 & 175\\ 1 & 13\end{matrix}\right)$ ← Πολλαπλασιάζουμε την πρώτη γραμμή με το 25^{-1} =25

$\left(\begin{matrix}1 & 0\\ 15 & 1\end{matrix}\middle|\begin{matrix}24 & 19\\ 1 & 13\end{matrix}\right)$ ← Αντικαθιστούμε τους αριθμούς με το υπόλοιπό τους modulo 26.

$\left(\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\middle|\begin{matrix}24 & 19\\ -359 & -272\end{matrix}\right)$ ← Πολλαπλασιάζουμε την πρώτη γραμμή με το -15 και την προσθέτουμε στην δεύτερη.

$\left(\begin{matrix}1 & 0\\ 0 & 1\end{matrix}\middle|\begin{matrix}24 & 19\\ 5 & 14\end{matrix}\right)$ ← Αντικαθιστούμε τους αριθμούς με το υπόλοιπό τους modulo 26.

Έτσι βρίσκουμε ότι

$$(A^{-1})^T = \begin{bmatrix}24 & 19\\ 5 & 14\end{bmatrix}$$

Άρα ο πίνακας αποκρυπτογράφησης είναι:

$$A^{-1} = \begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}$$

Για την αποκρυπτογράφηση ολόκληρου του μηνύματος , χωρίζουμε το μήνυμα σε ζευγάρια γραμμάτων και βρίσκουμε από τον πίνακα 1 τα αριθμητικά ισοδύναμα των γραμμάτων.

LN	GI	HG	YB	VR	EN	JY	QO
12 14	7 9	8 7	25 2	22 18	5 14	10 25	17 15

Μετά, πολλαπλασιάζουμε διαδοχικά τα κωδικοποιημένα διανύσματα που βρήκαμε παραπάνω με τον A^{-1} από αριστερά,

$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}12\\ 14\end{bmatrix} = \begin{bmatrix}358\\ 424\end{bmatrix} = \begin{bmatrix}20\\ 8\end{bmatrix}$ (mod26) $\begin{matrix}T\\ H\end{matrix}$

$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}7\\ 9\end{bmatrix} = \begin{bmatrix}213\\ 259\end{bmatrix} = \begin{bmatrix}5\\ 25\end{bmatrix}$ (mod26) $\begin{matrix}E\\ Y\end{matrix}$

$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}8\\ 7\end{bmatrix} = \begin{bmatrix}227\\ 250\end{bmatrix} = \begin{bmatrix}19\\ 16\end{bmatrix}$ (mod26) $\begin{matrix}S\\ P\end{matrix}$

$$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}25\\ 2\end{bmatrix} = \begin{bmatrix}610\\ 503\end{bmatrix} = \begin{bmatrix}12\\ 9\end{bmatrix} \pmod{26} \quad \begin{matrix}L\\ I\end{matrix}$$

$$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}22\\ 18\end{bmatrix} = \begin{bmatrix}618\\ 670\end{bmatrix} = \begin{bmatrix}20\\ 20\end{bmatrix} \pmod{26} \quad \begin{matrix}T\\ T\end{matrix}$$

$$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}5\\ 14\end{bmatrix} = \begin{bmatrix}190\\ 291\end{bmatrix} = \begin{bmatrix}8\\ 5\end{bmatrix} \pmod{26} \quad \begin{matrix}H\\ E\end{matrix}$$

$$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}10\\ 25\end{bmatrix} = \begin{bmatrix}365\\ 540\end{bmatrix} = \begin{bmatrix}1\\ 20\end{bmatrix} \pmod{26} \quad \begin{matrix}A\\ T\end{matrix}$$

$$\begin{bmatrix}24 & 5\\ 19 & 14\end{bmatrix}\begin{bmatrix}17\\ 15\end{bmatrix} = \begin{bmatrix}483\\ 533\end{bmatrix} = \begin{bmatrix}15\\ 13\end{bmatrix} \pmod{26} \quad \begin{matrix}O\\ M\end{matrix}$$

Από τον πίνακα 4 και τα αλφαβητικά ισοδύναμα έχουμε:

THEYSPLITTHEATOM

THEY SPLIT THE ATOM

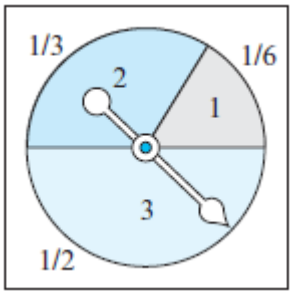
3 ΚΕΦΑΛΑΙΟ ΘΕΩΡΙΑ ΠΑΙΓΝΙΩΝ

3.1 Εισαγωγή

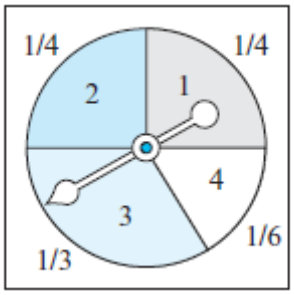
Η Θεωρία παιγνίων ασχολείται με τη μαθηματική μοντελοποίηση των παιγνίων.
Λέγοντας παίγνιο θα εννοούμε ένα συγκεκριμένο σύνολο από παίχτες, κανόνες και ένα καθορισμένο τρόπο πληρωμής για κάθε αποτέλεσμα που θα προκύπτει από την εφαρμογή του παίγνιου από τους παίκτες.
Ο όρος παιχνίδι θα δηλώνει συγκεκριμένη εφαρμογή του παίγνιου (παρτίδα).
Θα μελετήσουμε μόνο παίγνια όπου συμμετέχουν μόνο δύο παίκτες και υποθέτουμε ότι οι συγκεκριμένοι τρόποι που παίζουν αυτοί οι δύο έχουν απαριθμηθεί.
Σε αυτό το κεφάλαιο θα μελετήσουμε ένα γενικό παιχνίδι στο οποίο δύο αντίπαλοι παίκτες διαλέγουν διαφορετικές στρατηγικές για να επιτύχουν το στόχο τους.
Η βέλτιστη τεχνική του κάθε παίκτη σε μερικές περιπτώσεις βρίσκεται με τη χρήση τεχνικών πινάκων.
Για να παρουσιάσουμε τη βασική έννοια της θεωρίας παιγνίων, θεωρούμαι το παρακάτω παίγνιο:

3.1.1 **Παίγνιο**

Δύο παίκτες, τους οποίους ονομάζουμε παίκτης Α και παίκτης Β έχουν αποφασίσει να παίξουν το παρακάτω παιχνίδι:
Κάθε παίκτης έχει έναν στατικό τροχό με έναν κινούμενο δείκτη όπως φαίνονται στην εικόνα 5



Τροχός- γραμμής του παίκτη Α



Τροχός – στήλης του παίκτη Β

Εικόνα 5 Παίγνιο 1

Θα ονομάσουμε τον τροχό του παίκτη Α τροχός – γραμμής και τον τροχό του παίκτη Β, τροχό – στήλης.
Ο τροχός γραμμής χωρίζεται σε τρεις τομείς, 1,2 και 3 και ο τροχός στήλης σε τέσσερις τομείς,1,2,3 και 4.
Τα μέρη του τροχού τα οποία περιέχονται σε κάθε τομέα φαίνονται στην εικόνα 5.
Για να παίξουν το παιχνίδι κάθε παίκτης γυρίζει τον δείκτη του τροχού του, ο οποίος σταματά σε κάποιον τομέα στην τύχη.
Ο αριθμός του συγκεκριμένου τομέα στον οποίο δείχνει ο δείκτης είναι η κίνηση του κάθε παίκτη. Έτσι ο παίκτης Α έχει τρεις διαφορετικές κινήσεις ενώ ο παίκτης Β έχει τέσσερις διαφορετικές κινήσεις.
Ανάλογα με τη κίνηση την οποία κάνει ο κάθε παίκτης, ο παίκτης Β πληρώνει τον παίκτη Α σύμφωνα με τον παρακάτω πίνακα 6.

		Κίνηση παίκτη Β			
		1	2	3	4
Κίνηση παίκτη Α	1	**3 €**	**5 €**	**-2 €**	**1 €**
	2	**-2 €**	**4 €**	**-3 €**	**-4 €**
	3	**6 €**	**-5 €**	**0 €**	**3 €**

Πίνακας 6 Πληρωμή στον παίκτη Α

Για παράδειγμα εάν ο δείκτης του τροχού - γραμμή ,παίκτης Α, σταματήσει στον τομέα 1 και ο δείκτης του τροχού- στήλη ,παίκτης Β, σταματήσει στον τομέα 2, τότε ο παίκτης Β πρέπει να πληρώσει στον παίκτη Α το ποσό των 5€.
Παρατηρούμε ότι κάποιες εγγραφές του πίνακα είναι αρνητικές, αυτό σημαίνει ότι ο παίκτης Α αντί να πληρώνεται από τον παίκτη Β , αντίθετα πληρώνει τον παίκτη Β.
Έτσι οι θετικές εγγραφές του πίνακα είναι κέρδη για τον παίκτη Α και ζημιά για τον παίκτη Β, ενώ οι αρνητικές εγγραφές του πίνακα είναι ζημιά για τον παίκτη Α και κέρδη για τον παίκτη Β.
Σε αυτό το παιχνίδι όπως καταλαβαίνουμε οι παίκτες δεν έχουν καμία άποψη για την κίνησή τους, όλα είναι θέμα τύχης.

3.2 Παίγνιο δύο ατόμων με μηδενικό άθροισμα κέρδους- ζημιάς.

Το παιχνίδι το οποίο περιέγραψα παραπάνω είναι ένα παράδειγμα ενός παιγνίου δύο ατόμων με μηδενικό άθροισμα κέρδους ζημιάς. Ο όρος μηδενικό άθροισμα κέρδους ζημιάς σημαίνει ότι σε κάθε παρτίδα του παιγνίου το κέρδος του ενός παίκτη είναι ίσο με τη ζημιά του άλλου. Έτσι το άθροισμα κέρδους ζημιάς είναι μηδέν.
Επειδή κάθε παίκτης έχει ένα πεπερασμένο πλήθος κινήσεων, όσες και οι επιλογές του, τα αποτελέσματα μπορούν να παρασταθούν με έναν πίνακα, όπως είναι ο πίνακας 6.
Γενικά στα παίγνια αυτού του τύπου έστω ότι ο παίκτης Α έχει m πιθανές κινήσεις και ο παίκτης Β έχει n πιθανές κινήσεις. Σε μια παρτίδα του παιγνίου, κάθε παίκτης κάνει μια από τις πιθανές του κινήσεις και ο παίκτης α κερδίζει κάποια πληρωμή από τον παίκτη Β.

3.2.1 **Ορισμός**

Για i = 1,2,…,m και j = 1,2,…,n ορίζουμε:

α_{ij} = Η πληρωμή κερδίζει ο παίκτης Α από τον παίκτη Β, όταν ο Α κάνει την κίνηση i και ο Β την κίνηση j.

Η πληρωμή΄ δεν είναι απαραίτητο να είναι χρήματα, μπορεί να είναι οτιδήποτε μπορεί να παρασταθεί με μια αριθμητική τιμή. Όπως προηγουμένως εάν μια εγγραφή α_{ij} είναι αρνητική , αυτό σημαίνει ότι ο παίκτης Α πληρώνει το ποσό $|\alpha_{ij}|$ στον παίκτη Β.
Ταξινομούμε αυτές τις mn πιθανές πληρωμές στον παρακάτω m×n πίνακα, ο οποίος ονομάζεται ***πίνακας πληρωμής του παιγνίου.***

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix}$$

Σημαντικό ρόλο παίζει η πιθανότητα με τη οποία ο κάθε παίκτης θα επιλέξει την κίνησή του. Για παράδειγμα για το παίγνιο 3.1.1. για το οποίο συζητήσαμε η αναλογία του εμβαδού του τομέα προς το εμβαδό όλου του δίσκου είναι η πιθανότητα με την οποία κάνει ο παίκτης την κίνησή του.

Δηλαδή σύμφωνα με την εικόνα 5. : ο παίκτης Α έχει πιθανότητα $\frac{1}{3}$ για το 2

ο παίκτης Β έχει πιθανότητα $\frac{1}{4}$ για το 2.

Στη γενική περίπτωση έχουμε τους παρακάτω ορισμούς:

p_i = Η πιθανότητα με την οποία ο παίκτης Α πετυχαίνει ή επιλέγει την i επιλογή (i = 1,2,…,m)

q_j = Η πιθανότητα με την οποία ο παίκτης Β πετυχαίνει ή επιλέγει την j επιλογή (j = 1,2,…,n)

Από τους παραπάνω ορισμούς προκύπτει ότι

$$p_1 + p_2 + \ldots + p_m = 1$$

και

$$q_1 + q_2 + \ldots + q_n = 1$$

Με τις πιθανότητες p_i και q_j δημιουργούμε δύο διανύσματα :

$$\text{p} = [p_1 \quad p_2 \quad \ldots \quad p_m] \qquad \text{και} \qquad \text{q} = \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_n \end{bmatrix}$$

3.2.2 **Ορισμός .**

Καλούμε το διάνυσμα γραμμή p , ***στρατηγική*** του παίκτη Α, και το διάνυσμα στήλη q *στρατηγική* του παίκτη Β.

Για παράδειγμα στο παίγνιο 3.1.1. έχουμε

$$\text{p} = \begin{bmatrix} \frac{1}{6} & \frac{1}{3} & \frac{1}{2} \end{bmatrix} \qquad \text{και} \qquad \text{q} = \begin{bmatrix} \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{3} \\ \frac{1}{6} \end{bmatrix}$$

Αν οι επιλογές των δύο παικτών είναι ανεξάρτητες μεταξύ τους, τότε $p_i q_j$ είναι η πιθανότητα να πετύχει ο παίκτης Α την Ι επιλογή και ο παίκτης Β την j επιλογή. Το τίμημα σε αυτήν την περίπτωση είναι α_{ij} και η πιθανότητα της τιμής αυτής είναι p_{ij}. Εάν πολλαπλασιάσουμε κάθε τίμημα με την αντίστοιχη πιθανότητά του και προσθέσουμε τα γινόμενα έχουμε άθροισμα:

$$\alpha_{11}p_1q_1 + \alpha_{12}p_1q_2 + \ldots + \alpha_{1n}p_1q_n + \alpha_{21}p_2q_1 + \ldots + \alpha_{2n}p_2q_n + \ldots + \alpha_{mn}p_mq_n$$

3.2.3 **Ορισμός .**

Το ανωτέρω άθροισμα δίνει το μέσο όρο του ποσού για τον παίκτη Α. Αυτή η τιμή καλείται ***Αναμενόμενη τιμή*** για τον παίκτη Α.
Είναι γνωστό ότι αν ένα παίγνιο επαναληφθεί πολλές φορές το αναμενόμενο κέρδος του παίκτη Α θα είναι ίσο με αυτό το άθροισμα.
Συμβολίζουμε την Αναμενόμενη Τιμή ως **E(p, q)** για να τονίσουμε το γεγονός ότι εξαρτάται από τη στρατηγική των δύο παικτών.
Από τον ορισμό του πίνακα πληρωμής του παιγνίου Α και τις στρατηγικές p και q , μπορεί να επαληθευθεί ότι μπορούμε να εκφράσουμε την Αναμενόμενη Τιμή ως:

$$E(p, q) = [p_1 \quad p_2 \quad \dots \quad p_m] \begin{bmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_n \end{bmatrix} = pAq$$

Επειδή E(p, q) είναι η αναμενόμενη πληρωμή στον παίκτη Α είναι επακόλουθο ότι η πληρωμή στον παίκτη Β είναι - E(p, q)

3.2.4 **Παράδειγμα**

Για το παίγνιο 3.1.1. έχουμε:

$$E(p, q) = pAq = \begin{bmatrix} \frac{1}{6} & \frac{1}{3} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 3 & 5 & -2 & 1 \\ -2 & 4 & -3 & -4 \\ 6 & -5 & 0 & 3 \end{bmatrix} \begin{bmatrix} \frac{1}{4} \\ \frac{1}{4} \\ \frac{1}{3} \\ \frac{1}{6} \end{bmatrix} = \frac{13}{72} = 0.1805$$

Έτσι μακροπρόθεσμα ο παίκτης Α θα λάβει 0,1805€ από τον παίκτη Β.

3.3 Παίγνια με επιλογή στρατηγικής.

Μέχρι τώρα έχουμε δει παίγνια στα οποία οι παίκτες έχουν προκαθορισμένη στρατηγική, Ας δούμε τώρα μια πιο δύσκολη περίπτωση, στην οποία οι δύο παίκτες μπορούν να αλλάξουν την στρατηγική τους ανεξάρτητα. Για παράδειγμα στο παίγνιο 3.1.1 επιτρέπεται στους δύο παίκτες να τροποποιήσουν τους τομείς των δεικτών των δίσκων τους έτσι ώστε να ελέγχουν τις πιθανότητες των αντίστοιχων κινήσεων. Αυτό αλλάζει ποιοτικά τη φύση του προβλήματος και μας βάζει για τα καλά στο πεδίο της πραγματικής θεωρία παιγνίων. Είναι κατανοητό ότι κάθε παίκτης δεν γνωρίζει τι στρατηγική θα ακολουθήσει ο αντίπαλος του. Επίσης είναι προϋπόθεση ότι ο κάθε παίκτης θα διαλέξει την καλύτερη στρατηγική για τον εαυτό του και ο αντίπαλος το ξέρει αυτό. Έτσι ο παίκτης Α προσπαθεί να επιλέξει μια στρατηγική p έτσι ώστε η Αναμενόμενη τιμή E(p, q) να είναι όσο μεγαλύτερη γίνεται για την καλύτερη στρατηγική q που θα επιλέξει ο παίκτη Β. Παρόμοια ο παίκτης Β προσπαθεί να επιλέξει μια στρατηγική q τέτοια ώστε η Αναμενόμενη Τιμή E(p, q) να είναι όσο μικρότερη γίνεται για την καλύτερη στρατηγική που θα διαλέξει ο παίκτης Α.
Για να δούμε ότι αυτές οι επιλογές είναι στην πραγματικότητα δυνατόν να πραγματοποιηθούν χρειαζόμαστε το παρακάτω θεώρημα το οποίο καλείται:

Θεμελιώδες Θεώρημα των παιγνίων δύο ατόμων με μηδενικό άθροισμα κέρδους-ζημιάς.

3.3.1 **Θεώρημα:**

Υπάρχουν στρατηγικές p^* και q^* έτσι ώστε :

$$E(p^*, q) \geq E(p^*, q^*) \geq E(p, q^*)$$

για όλες τις στρατηγικές p και q.

Σε αυτό το θεώρημα οι στρατηγικές p^* και q^* είναι οι καλύτερες δυνατές στρατηγικές για τους παίκτες Α και Β αντίστοιχα. Έστω $u = E(p^*, q^*)$ τότε $E(p^*, q) \geq u$ για κάθε στρατηγική q.

Αυτό σημαίνει ότι εάν ο παίκτης Α επιλέξει τη στρατηγική p^* τότε ανεξάρτητα ποια στρατηγική q θα διαλέξει ο παίκτης Β η αναμενόμενη πληρωμή στον παίκτη Α δεν θα πέσει ποτέ κάτω από τη u. Δηλαδή το ποσό που θα κερδίσει ο Α θα είναι μεγαλύτερο ή ίσο του u.

Για τον παίκτη Β έχουμε $u \geq E(p, q^*)$ για κάθε στρατηγική p που θα επιλέξει ο παίκτης Α. Το κέρδος του παίκτη Β δίνεται από

$E(p^*, q^*) \geq E(p, q^*) \Rightarrow -E(p, q^*) \geq -E(p^*, q^*)$ για κάθε p .

Άρα ο παίκτης Β θα πληρώσει μέχρι u αν επιλέξει την στρατηγική q^* ανεξάρτητα ποια στρατηγική p θα ακολουθήσει ο παίκτης Α.

3.3.2 **Ορισμός .**

Εάν p^* και q^* είναι στρατηγικές τέτοιες ώστε:

$$E(p^*, q) \geq q^* \geq E(p, q^*)$$

για όλες τις στρατηγικές p και q τότε:

i) η p^* καλείται η *βέλτιστη στρατηγική* για τον παίκτη Α
ii) η q^* καλείται η *βέλτιστη στρατηγική* για τον παίκτη Β
iii) η $u = E(p^*, q^*)$ καλείται *τιμή* του παιγνίου.

Η διατύπωση σε αυτόν τον ορισμό υπονοεί ότι οι βέλτιστες στρατηγικές δεν είναι απαραίτητα μοναδικές. Αλλά όλες οι βέλτιστες στρατηγικές δίνουν τη ίδια τιμή παιγνίου. Έτσι εάν p^*, q^* και p^{**} , q^{**} είναι βέλτιστες στρατηγικές τότε

$$E(p^*, q^*) = E(p^{**}, q^{**})$$

Συνεπώς η τιμή του παίγνιου είναι το αναμενόμενο κέρδος του παίκτη Α, όταν και οι δύο παίκτες επιλέγουν τη βέλτιστη στρατηγική,

Για να βρούμε τις βέλτιστες στρατηγικές πρέπει να βρούμε τα διανύσματα p^* και q^* τα οποία ικανοποιούν την εξίσωση

$$E(p^*, q) \geq q^* \geq E(p, q^*) .$$

Για να βρεθούν οι βέλτιστες στρατηγικές γενικά χρησιμοποιούμε τεχνικές Γραμμικού Προγραμματισμού, αλλά έχουμε μερικές ειδικές περιπτώσεις που μπορούμε να βρούμε τις βέλτιστες στρατηγικές με πιο στοιχειώδεις τεχνικές.

3.4 Εύρεση βέλτιστης στρατηγικής με χρήση Σαγματικού Σημείου.

3.4.1 **Ορισμός .**

Ένα στοιχείο a_{rs} του πίνακα πληρωμής Α καλείται ***Σαγματικό Σημείο*** εάν

i. η a_{rs} είναι η μικρότερη τιμή στη γραμμή της, δηλαδή $a_{rj} \geq a_{rs}$ ∀ j
ii. η a_{rs} είναι η μεγαλύτερη τιμή στη στήλη της δηλαδή $a_{is} \leq a_{rs}$ ∀ i.

Ένα παίγνιο του οποίου ο πίνακας πληρωμής Α έχει σαγματικό σημείο καλείται ***αυστηρά καθορισμένο***.

Για παράδειγμα το χρωματισμένο στοιχείο στους παρακάτω πίνακες είναι σαγματικό σημείο.

$$\begin{bmatrix} 3 & 1 \\ -4 & 0 \end{bmatrix} \qquad \begin{bmatrix} 30 & -50 & -5 \\ 60 & 90 & 75 \\ -10 & 60 & -30 \end{bmatrix} \qquad \begin{bmatrix} 0 & -3 & 5 & -9 \\ 15 & -8 & -2 & 10 \\ 7 & 10 & 6 & 9 \\ 6 & 11 & -3 & 2 \end{bmatrix}$$

Εάν ένας πίνακας έχει Σαγματικό σημείο a_{rs} προκύπτει ότι οι ακόλουθες στρατηγικές είναι βέλτιστες:

$$p^* = [0 \quad 0 \quad \dots \quad 1 \quad \dots \quad 0] \qquad q^* = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} s$$

r

Έτσι η βέλτιστη στρατηγική για τον παίκτη Α είναι να κάνει την r κίνηση ενώ για τον παίκτη Β είναι να κάνει την s κίνηση.
Τέτοιες στρατηγικές στις οποίες μόνο μια κίνηση είναι δυνατή ονομάζονται ***απλές στρατηγικές***.
Στρατηγικές στις οποίες περισσότερες από μια κινήσεις είναι πιθανές ονομάζονται ***ανάμεικτες στρατηγικές***.
Για να δούμε ότι παραπάνω στρατηγικές είναι βέλτιστες αρκεί να επιβεβαιώσουμε τις παρακάτω εξισώσεις:

$$E(p^*, q^*) = p^* A\, q^* = a_{rs}$$
$$E(p^*, q) = p^* A\, q \geq a_{rs} \quad \text{για κάθε στρατηγική q}$$
$$E(p, q^*) = p\, A\, q^* \leq a_{rs} \quad \text{για κάθε στρατηγική p}$$

Και οι τρεις εξισώσεις μαζί συνεπάγονται ότι :

$$E(p^*, q) \geq E(p^*, q^*) \geq E(p, q^*)$$

Για όλες τις στρατηγικές p και q. Άρα σύμφωνα με το θεώρημα 3.3.1 οι στρατηγικές p^* και q^* είναι βέλτιστες.

Από τα παραπάνω συμπεραίνουμε ότι η τιμή ενός αυστηρά καθορισμένου παίγνιου είναι η αριθμητική τιμή του σαγματικού σημείου a_{rs}.

Είναι πιθανόν ένας πίνακας πληρωμής να έχει αρκετά σαγματικά σημεία, αλλά τότε η μοναδικότητα της τιμής του παιγνίου εγγυάται ότι όλα τα σαγματικά σημεία θα έχουν την ίδια αριθμητική τιμή.

3.4.2 **Παράδειγμα.**

Έστω ότι ο πίνακας πληρωμής του παίγνιου είναι ο ακόλουθος:

$$\begin{array}{c} \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{bmatrix} -5 & 11 & -7 \\ -2 & 8 & -1 \\ -3 & -4 & 14 \end{bmatrix} \end{array}$$

Ας υποθέσουμε ότι και οι δύο παίζουν αμυντικά, δηλαδή να αποφύγουν το χειρότερο. Για τον Α το χειρότερο της πρώτης στρατηγικής (γραμμή) είναι το -7, της δεύτερης το -2 και της τρίτης το -4. Από αυτά το καλύτερο είναι το -2. Για τον Β παίκτη έχουμε το χειρότερο της πρώτης στρατηγικής (στήλη) είναι το 2, της δεύτερης είναι το -11 και της τρίτης το -14. Υπενθυμίζουμε ότι οι πληρωμές του Β παίκτη είναι αντίθετες από τις πληρωμές του Α παίκτη. Το καλύτερο από τα χειρότερα είναι το 2 το οποίο αντιστοιχεί στο στοιχείο a_{21}του πίνακα , το οποίο είναι σαγματικό σημείο.
Η επιλογή αυτή έχει μεγάλη σταθερότητα και αν κάποιος από τους παίκτες ξεφύγει από αυτήν την επιλογή πιθανόν θα εξαναγκαστεί να επανέλθει. Η σταθερότητα οφείλεται στην ακόλουθη εξίσωση:

Το maximum των minimum του Α = - Το maximum των minimum του Β.

Αν το παίγνιο έχει αυτή την ιδιότητα , ο πίνακας του έχει σαγματικό σημείο.

3.4.3 **Παράδειγμα Βέλτιστες στρατηγικές για την μεγιστοποίηση της τηλεθέασης.**

Δύο αντίπαλοι τηλεοπτικοί σταθμοί ο ΑΛΦΑ και ο ΒΗΤΑ προγραμματίζουν μια ωριαία εκπομπή τη ίδια χρονική περίοδο. Ο ΑΛΦΑ έχει επιλογή από τρία διαφορετικά προγράμματα και ο ΒΗΤΑ από τέσσερα. Κανένας σταθμός δεν ξέρει ποιο πρόγραμμα σχεδιάζει ο αντίπαλος. Και οι δύο σταθμοί ανέθεσαν σε μια εταιρεία να τους δώσει μια εκτίμηση της τηλεθέασης για όλα τα δυνατά ζεύγη προγραμμάτων.
Η εταιρεία τους έδωσε τον ακόλουθο πίνακα ο οποίος εκφράζει την τηλεθέαση του σταθμού ΑΛΦΑ. Δηλαδή το στοιχείο a_{ij} δείχνει το ποσοστό της τηλεθέασης του σταθμού ΑΛΦΑ όταν ο ΑΛΦΑ έχει το πρόγραμμα I και ο ΒΗΤΑ το πρόγραμμα j.

		Πρόγραμμα σταθμού ΒΗΤΑ			
		1	2	3	4
Πρόγραμμα σταθμού ΑΛΦΑ	1	60	20	30	55
	2	50	75	45	60
	3	70	45	35	30

Πίνακας 7 Πίνακας τηλεθέασης

Ποιο πρόγραμμα θα δώσει το μεγαλύτερο ακροατήριο σε κάθε σταθμό;

Θεωρούμε το πρόβλημα αυτό, παίγνιο με δύο παίκτες μηδενικού αθροίσματος κέρδους-ζημιάς και ο πίνακας του παιγνίου είναι ο ακόλουθος.

$$A = \begin{bmatrix} 10 & -30 & -20 & 5 \\ 0 & 25 & -5 & 10 \\ 20 & -5 & -15 & -20 \end{bmatrix}$$

Τον πίνακα αυτόν τον κατασκευάσαμε αφαιρώντας 50 από κάθε στοιχείο του πίνακα που έδωσε η εταιρεία στους δύο τηλεοπτικούς σταθμούς.
Θεωρούμε ότι και οι δύο σταθμοί ξεκινούν με το 50% της τηλεθέασης και το στοιχείο a_{ij} είναι το ποσοστό της τηλεθέασης που κερδίζει ο σταθμός ΑΛΦΑ και χάνει ο σταθμός ΒΗΤΑ εάν το πρόγραμμα ι είναι απέναντι στο πρόγραμμα j.

Είναι εύκολο να δούμε ότι το στοιχείο

$$a_{23} = -5$$

είναι σαγματικό σημείο του πίνακα πληρωμής.

Άρα η βέλτιστη στρατηγική του σταθμού ΑΛΦΑ είναι το πρόγραμμα 2 και η βέλτιστη στρατηγική του σταθμού ΒΗΤΑ είναι το πρόγραμμα 3.

Αυτό έχει ως αποτέλεσμα ο σταθμός ΑΛΦΑ να έχει τηλεθέαση 45%, άρα ο σταθμός Β θα έχει τηλεθέαση 55%.

3.5 Εύρεση βέλτιστης στρατηγικής με χρήση πίνακα 2×2.

Άλλη μία περίπτωση στην οποία οι βέλτιστες στρατηγικές μπορούν να βρεθούν με βασικές γνώσεις είναι η περίπτωση στην οποία κάθε παίκτης έχει μόνο δύο πιθανές κινήσεις. Σε αυτήν την περίπτωση ο πίνακας πληρωμής είναι ένας πίνακας 2×2.

$$A = \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix}$$

Εάν ο παίγνιο είναι αυστηρά καθορισμένο, τότε τουλάχιστον μια εγγραφή από τις τέσσερις του πίνακα είναι σαγματικό σημείο και μπορούμε να εφαρμόσουμε την τεχνική που αναπτύξαμε παραπάνω για την εύρεση των βέλτιστων στρατηγικών.
Εάν το παίγνιο δεν είναι αυστηρά καθορισμένο, πρώτα υπολογίζουμε την αναμενόμενη πληρωμή για τυχαίες στρατηγικές p και q.

$$E(p,q) = pAq = [p_1 \quad p_2] \begin{bmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \end{bmatrix} =$$
$$= a_{11}p_1q_1 + a_{12}p_1q_2 + a_{21}p_2q_1 + a_{22}p_2q_2 \qquad (1)$$

Και επειδή

$$p_1+p_2 = 1 \text{ και } q_1+q_2 = 1$$

Μπορούμε να αντικαταστήσουμε στην (1)

$$p_2 = 1 - p_1 \quad \text{και} \quad q_2 = 1 - q_1$$

και έχουμε:

$$E(p,q) = a_{11}p_1q_1 + a_{12}p_1(1 - q_1) + a_{21}(1 - p_1)q_1 + a_{22}(1 - p_1)(1 - q_1) =$$
$$= a_{11}p_1q_1 + a_{12}p_1 + a_{12}p_1q_1 + a_{21}q_1 - a_{21}p_1q_1 + a_{22} - a_{22}q_1 - a_{22}p_1 + a_{22}p_1q_1$$
$$\Leftrightarrow$$
$$E(p,q) = [(a_{11} + a_{22} - a_{12} - a_{21})p_1 - (a_{22} - a_{21})]q_1 + (a_{12} - a_{22})p_1 + a_{22} \qquad (2)$$

Εξετάζοντας τον συντελεστή του όρου q_1 στη (2) βλέπουμε ότι εάν θέσουμε:

$$p_1 = p_1^* = \frac{a_{22} - a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} \qquad (3)$$

τότε ο συντελεστής γίνεται μηδέν και η (2) απλοποιείται :

$$E(p^*, q) = 0q_1 + (a_{12} - a_{22}) \frac{a_{22} - a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} + a_{22}$$

$\Leftrightarrow$

$$E(p^*, q) = \frac{a_{11}a_{22} - a_{12}a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} \quad (4)$$

Η εξίσωση (4) είναι ανεξάρτητη από τη στρατηγική q , έτσι εάν ο παίκτης Α επιλέξει τη στρατηγική του $p^* = [p_1^*, 1- p_1^*]$ τότε ο παίκτης Β δεν μπορεί να αλλάξει την τιμή του παιγνίου διαφοροποιώντας τη στρατηγική του.

Αντίστοιχα μπορεί να επαληθευθεί ότι εάν ο παίκτης Β επιλέξει τη στρατηγική:

$$q_1 = q_1^* = \frac{a_{22} - a_{12}}{a_{11} + a_{22} - a_{12} - a_{21}} \quad (5)$$

τότε η αντικατάσταση στην (2) δίνει:

$$E(p, q^*) = \frac{a_{11}a_{22} - a_{12}a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} \quad (6)$$

Οι ισότητες (4) και (6) μας δίνουν:

$$E(p^*, q) = E(p^*, q^*) = E(p, q^*) \quad (7)$$

για όλες τις στρατηγικές p και q.

Άρα σύμφωνα με τον ορισμό οι παραπάνω στρατηγικές (3) και (5) είναι βέλτιστες.

3.5.1 **Θεώρημα .**

Για ένα παίγνιο με πίνακα 2×2 που δεν είναι αυστηρά καθορισμένο , οι βέλτιστες στρατηγικές για τους δύο παίκτες είναι:

$$p^* = \left[\frac{a_{22} - a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} \quad \frac{a_{11} - a_{12}}{a_{11} + a_{22} - a_{12} - a_{21}}\right]$$

$$q^* = \begin{bmatrix} \frac{a_{22} - a_{12}}{a_{11} + a_{22} - a_{12} - a_{21}} \\ \frac{a_{11} - a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} \end{bmatrix}$$

και η τιμή του παιγνίου είναι :

$$E = \frac{a_{11}a_{22} - a_{12}a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}}$$

3.5.2 **Εφαρμογή**

Το Υπουργείο Υγείας επιθυμεί να εμβολιάσει τους πολίτες εναντίον ενός ιού. Ο ιός έχει δύο μεταλλάξεις και δεν είναι γνωστό με τι αναλογία οι μεταλλάξεις αυτές εμφανίζονται. Δύο εμβόλια έχουν αναπτυχθεί με διαφορετικές δράσεις εναντίον των δύο μεταλλάξεων. Το εμβόλιο 1 είναι 85% αποτελεσματικό εναντίον της μετάλλαξης Γ και 70% εναντίον της μετάλλαξης Δ. Το εμβόλιο 2 είναι 60% αποτελεσματικό εναντίον της μετάλλαξης Γ και 90% εναντίον της μετάλλαξης Δ. Ποιος είναι ο καλύτερος εμβολιασμός;

Θα αντιμετωπίσουμε αυτό το πρόβλημα σαν ένα παίγνιο δύο παικτών όπου ο παίκτης Α δηλαδή η κυβέρνηση επιθυμεί να κάνει την πληρωμή, την αποτελεσματικότητα του εμβολιασμού , όσο το δυνατόν μεγαλύτερη. Ο παίκτης Β δηλαδή ο ιός επιθυμεί να κάνει την πληρωμή όσο το δυνατόν μικρότερη.

Ο πίνακας είναι ο παρακάτω:

		Ιός	
		Γ	***Δ***
Εμβόλιο	***Γ***	0.85	0,70
	Δ	0,60	0,90

Ο πίνακας δεν έχει σαγματικό Σημείο άρα μπορούμε να εφαρμόσουμε το Θεώρημα 3.5.1. Συνεπώς:

$$p_1^* = \frac{a_{22} - a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} = \frac{0,90-0,60}{0,85+0,90-0,70-0,60} = \frac{0,30}{0,45} = \frac{2}{3}$$

$$p_2^* = 1 - p_1^* = 1 - \frac{2}{3} = \frac{1}{3}$$

$$q_1^* = \frac{a_{22} - a_{12}}{a_{11} + a_{22} - a_{12} - a_{21}} = \frac{0,90-0,70}{0,85+0,90-0,70-0,60} = \frac{0,20}{0,45} = \frac{4}{9}$$

$$q_2^* = 1 - q_1^* = 1 - \frac{4}{9} = \frac{5}{9}$$

$$E = \frac{a_{11}a_{22} - a_{12}a_{21}}{a_{11} + a_{22} - a_{12} - a_{21}} = \frac{0,85\cdot 0,90-0,70\cdot 0,60}{0,85+0,90-0,70-0,60} = \frac{0,345}{0,45} = 0,76666666$$

Άρα η βέλτιστη στρατηγική για την κυβέρνηση είναι να εμβολιάζονται τα $\frac{2}{3}$ του πληθυσμού με το εμβόλιο 1 για τη μετάλλαξη Γ και το $\frac{1}{3}$ του πληθυσμού με το εμβόλιο 2 για τη μετάλλαξη Δ. Αυτό θα έχει ως αποτέλεσμα τουλάχιστον το 76,7% του πληθυσμού να μπορεί να αντισταθεί στον ιό ανεξάρτητα από την κατανομή των μεταλλάξεων. Επίσης μια κατανομή του ιού, $\frac{4}{9}$ της μετάλλαξης Γ και $\frac{5}{9}$ της μετάλλαξης Δ θα έχει σαν αποτέλεσμα το πολύ 76,7% του πληθυσμού να έχει αντίσταση στον ιό ανεξάρτητα της πολιτικής του εμβολιασμού που θα ακολουθήσει η κυβέρνηση.

Βιβλιογραφία

Ακολουθούν οι βιβλιογραφικές αναφορές (πηγές) της Εργασίας.

Howard Anton – Chris Rorres (2014) *Elementary Linear Algebra Application Version 11th Edition* Wiley.

Τρύφων Ι. Δάρας – Παναγώτης Σύψας (2003) *Στοχαστικές Ανελίξεις Θεωρία και Εφαρμογές*. Εκδόσεις Ζήτη

Νώντας Κεχαγιάς (2008) *Εφαρμογές της Γραμμικής Άλγεβρας* Προσπελάστηκε 04/05/2022

Μιχαήλ Ανούσης (2022) *Σημειώσεις παραδόσεων.*

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης.