Η Ανάλυση της Πληροφορίας, η Πληροφορική και η Θεωρία Πινάκων

Π. Πολυχρονίδου

Μαθηματικός-Διδάκτωρ Πληροφορικής, Επιστημονική Συνεργάτιδα του
Τ.Ε.Ι. Καβάλας, Τμήμα Λογιστικής, polychr@sdo.teikav.edu.gr

Περίληψη

Η ανάγκη της επεξεργασίας και της ανάλυσης της πολύπλοκης πληροφορίας οδηγεί την πληροφορική σε ολοένα και πιο βαθιά σύνδεσή της με τα μαθηματικά. Στην παρούσα εργασία παρουσιάζεται μία κλάση αραιών πινάκων που δημιουργεί έναν γραμμικό και έναν μη γραμμικό μετασχηματισμό κατάλληλους για κωδικοποίηση/συμπίεση της πληροφορίας και τη δημιουργία ενός κρυπτογραφικού αλγόριθμου, αντίστοιχα. Με επίδειξη των ανωτέρω στους μαθητές του Λυκείου μπορούμε να κεντρίσουμε το ενδιαφέρον τους, αφενός για τα μαθηματικά που δυσκολεύονται να κατανοήσουν, επιδεικνύοντας την συνεισφορά στους στην πληροφορική και αφετέρου για κάποια από τα προβλήματα που αντιμετωπίζουν σήμερα οι ερευνητές.

Λέξεις κλειδιά: *αραιοί πίνακες, γραμμικός μετασχηματισμός, μη γραμμικός μετασχηματισμός.*

Abstract

The need of processing and analyzing complex information leads informatics to connect more and more to mathematics. In this work we present a class of sparse matrices that generates a linear and a non linear transform, capable of coding/compressing information and creating a cryptographic algorithm, respectively. By demonstrating these properties to our students we can stimulate their interest firstly in mathematics, that they find it hard to understand, by demonstrating its contribution to informatics and secondly by showing them some of the problems that researchers have to deal with.

Keywords: *sparse matrices, linear transform, non linear transform.*

1. Εισαγωγή

Στις μέρες μας οι ερευνητές συχνά συναντούν το πρόβλημα της ανάκτησης, της αποθήκευσης και της επεξεργασίας της πληροφορίας. Για τον χαρακτηρισμό και τη μοντελοποίηση πολύπλοκων δεδομένων όπως για παράδειγμα είναι τα βιολογικά, τα ιατρικά και τα γλωσσολογικά, απαιτούνται καινούρια υπολογιστικά μαθηματικά, που να διαχειρίζονται την πληροφορία πολύπλοκων δεδομένων.

Προς αυτήν την κατεύθυνση η χρήση μεγάλων ψηφιακών βιβλιοθηκών έχει μεταμορφώσει δραματικά την επεξεργασία της πληροφορίας. Επειδή τα δεδομένα αποθηκεύονται συνήθως σε πίνακες, η Θεωρία Πινάκων έχει συμβάλλει σημαντικά

στην ανάπτυξη μεθόδων κωδικοποίησης, ταξινόμησης και ανάκτησης δεδομένων, έτσι ώστε να επιτυγχάνεται αφ' ενός κέρδος χωρητικότητας και αφ' ετέρου ταχεία υπολογιστική ικανότητα, βλ. (Berry, Drmac & Jessup, 1999). Ως εκ τούτου, ο ρόλος των αραιών πινάκων είναι πολύ σημαντικός, βλ. (Dongarra, 2000). Αραιός πίνακας (sparse matrix) είναι ένας πίνακας με μικρό αριθμό μη μηδενικών στοιχείων. Επομένως, με τη χρήση του εξοικονομείται χώρος αποθήκευσης στην μνήμη και οι υπολογισμοί γίνονται ταχύτερα.

Στην παρούσα εργασία επιδεικνύεται η μορφή μίας ευρείας κλάσης τετραγωνικών αντιστρέψιμων αραιών πινάκων. Οι πίνακες αυτοί προκύπτουν από έναν αρχικό πίνακα, όπου με επεξεργασία αναπαραγωγής/συρραφής σε πολλαπλά αντίγραφα οι παραγόμενοι νέοι πίνακες διατηρούν μερικές βασικές ιδιότητες του αρχικού. Με τον τρόπο αυτό δημιουργείται μία κλιμακωτή ανάλυση που εξασφαλίζει τον έλεγχο της τοπικής πληροφορίας. Έτσι, για παράδειγμα ένας πίνακας διάστασης *3 x 3* μπορεί να αναπτυχθεί σε πίνακες διάστασης $3^n \; x \; 3^n$, $n = 2, 3,..$ και επομένως μία ακολουθία δεδομένων μήκους 3^n, μπορεί να κωδικοποιηθεί/συμπιεσθεί σε μία ακολουθία με 3^k το πλήθος δεδομένα, όπου $k<n$, και εξ' αιτίας του ότι οι πίνακες αυτοί είναι αραιοί, επιτυγχάνεται μία ταχεία κωδικοποίηση/συμπίεση της τοπικής πληροφορίας.

Σκοπός της παρούσας εργασίας είναι να συνδυάσει το μάθημα «Ανάπτυξη Εφαρμογών σε Προγραμματιστικό Περιβάλλον» της Γ΄ Τάξης Τεχνολογικής Κατεύθυνσης Ενιαίων Λυκείων με τη σύγχρονη πραγματικότητα των ερευνητών. Είναι ανάγκη να επιδείξουμε στους μαθητές ότι οι γνώσεις που αποκτούν στο σχολείο, είναι η βάση για τις περισσότερες επιστήμες και επιπλέον αν αυτές συνδυαστούν κατάλληλα τότε μπορούν να συμβάλλουν στην εξέλιξη της επιστήμης.

Συγκεκριμένα, στην πρώτη παράγραφο, παρουσιάζεται η μορφή των αραιών πινάκων με την χρήση ενός χαρακτηριστικού παραδείγματος αυτών. Στη δεύτερη παράγραφο, παρουσιάζεται ο γραμμικός μετασχηματισμός αυτών στον χώρο των πεπερασμένων ακολουθιών και επιδεικνύεται ο τρόπος με τον οποίο κωδικοποιείται η πληροφορία. Στην τρίτη παράγραφο, παρουσιάζεται ο μη γραμμικός μετασχηματισμός που δημιουργείται από τους πίνακες και το γινόμενο Riesz και προτείνεται η χρησιμοποίηση αυτού στην κρυπτογραφία. Τέλος, στην τέταρτη παράγραφο, παρατίθενται τα συμπεράσματα που προκύπτουν από την παρούσα εργασία.

Πρέπει να σημειωθεί ότι η κλάση των αραιών πινάκων παρουσιάσθηκε στο περιοδικό SIAM Journal On Matrix Analysis and Applications, βλ. (Atreas, Karanikas & Polychronidou, 2008). Επίσης, στο περιοδικό Numerical Functional Analysis and Optimization, βλ. (Atreas & Polychronidou, 2008) αναπτύχθηκε μία μέθοδος πρόβλεψης ακολουθιών η οποία βασίζεται σε ιδιότητες της κλάσης των αραιών πινάκων.

2.1 Οι αραιοί πίνακες

Στην παράγραφο αυτή επιδεικνύεται η μορφή των πινάκων της κλάσης τετραγωνικών αντιστρέψιμων αραιών πινάκων. Έστω *m, N* είναι θετικοί ακέραιοι και $m = p_1 p_2 ... p_N$, $p_1 \geq p_2 \geq ... \geq p_N$, είναι η ανάλυση του *m* σε γινόμενο πρώτων παραγόντων. Κάθε στοιχείο U^m της κλάσης είναι πίνακας διάστασης *m x m* και τα μη μηδενικά στοιχεία του είναι ίσα με *1*. Κάθε πίνακας U^m κατασκευάζεται με μία αναδρομική διαδικασία *N* βημάτων, όσο είναι το πλήθος των πρώτων παραγόντων του *m*, με την χρήση τελεστών διαστολής και σύνθεσης πινάκων.

Παράδειγμα: Έστω $m = 12$, δηλαδή $p_1 = 3, p_2 = 2, p_3 = 2$ και $N = 3$. Η αναδρομική διαδικασία κατασκευής του πίνακα U^{12} είναι η εξής: Πρώτα, κατασκευάζεται ένας πίνακας *3x3*, όπου η πρώτη γραμμή έχει όλα τα στοιχεία της ίσα με *1* και υπόλοιπες *2* γραμμές είναι οι πρώτες *2* γραμμές του μοναδιαίου πίνακα *3x3*, δηλαδή:

$$U^{12}(1) = \begin{pmatrix} 1 & 1 & 1 \\ \hline 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Στο επόμενο βήμα, κατασκευάζεται ένας πίνακας *6x6*, όπου οι πρώτες *3* γραμμές είναι η διαστολή/μεγέθυνση κατά στήλες του πίνακα $U^{12}(1)$, δηλαδή παρατίθενται οι στήλες του πίνακα $U^{12}(1)$ δύο φορές η κάθε μία. Οι υπόλοιπες *3* γραμμές είναι η πρώτη γραμμή του μοναδιαίου πίνακα *2x2*, κατάλληλα μετατιθέμενη, δηλαδή:

$$U^{12}(2) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Στο τελευταίο βήμα, κατασκευάζουμε έναν πίνακα *12x12*, όπου οι πρώτες *6* γραμμές είναι η διαστολή/μεγέθυνση κατά στήλες του πίνακα $U^{12}(2)$, δηλαδή παρατίθενται οι στήλες του πίνακα $U^{12}(2)$ δύο φορές η κάθε μία. Οι υπόλοιπες *6* γραμμές είναι η πρώτη γραμμή του μοναδιαίου πίνακα *2x2*, κατάλληλα μετατιθέμενη, δηλαδή:

$$U^{12}(3)=\left(\begin{array}{cccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0\\
\hline
1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0
\end{array}\right).$$

2.2 Ο γραμμικός μετασχηματισμός των αραιών πινάκων

Έστω V_m είναι ο χώρος των πεπερασμένων ακολουθιών μήκους m, όπου ο m ικανοποιεί τη σχέση $m = p_1 p_2 ... p_N$, όπου $p_1,..,p_N$ είναι οι πρώτοι παράγοντες του m, τότε ο γραμμικός μετασχηματισμός $T : V_m \to V_m : t \to U^m t$ των πινάκων κωδικοποιεί την τοπική πληροφορία σε διάφορα επίπεδα κλιμάκωσης. Παραδείγματος χάριν, για *m=12*, έχουμε:

$$\left(\begin{array}{cccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&1&1&0&0&0&0\\
1&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&1&0&0\\
1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&1&0
\end{array}\right)\cdot\left(\begin{array}{c}t_1\\t_2\\t_3\\t_4\\t_5\\t_6\\t_7\\t_8\\t_9\\t_{10}\\t_{11}\\t_{12}\end{array}\right)=\left(\begin{array}{c}t_1+t_2+t_3+t_4+t_5+t_6+t_7+t_8+t_9+t_{10}+t_{11}+t_{12}\\t_1+t_2+t_3+t_4\\t_5+t_6+t_7+t_8\\t_1+t_2\\t_5+t_6\\t_9+t_{10}\\t_1\\t_3\\t_5\\t_7\\t_9\\t_{11}\end{array}\right).$$

Η κωδικοποίηση/συμπίεση της πληροφορίας επιτυγχάνεται με την εξής έννοια: Το πρώτο στοιχείο του μετασχηματισμού είναι ο μέσος όρος της πληροφορίας, το δεύτερο και τρίτο στοιχείο είναι η πληροφορία συμπιεσμένη σε τετράδες, τα στοιχεία

από το τέταρτο ως το έκτο είναι η πληροφορία συμπιεσμένη σε δυάδες και τα υπόλοιπα έξι στοιχεία είναι κατάλληλα επιλεγμένα στοιχεία της πληροφορίας. Δηλαδή, έχοντας τα πρώτα 3 στοιχεία του μετασχηματισμού υπολογίζεται η τρίτη τετράδα που δεν εμφανίζεται, δηλαδή το άθροισμα $t_9+ t_{10}+ t_{11}+ t_{12}$. Έχοντας τα πρώτα 6 στοιχεία του μετασχηματισμού υπολογίζονται οι τρεις δυάδες που δεν εμφανίζονται, δηλαδή τα αθροίσματα $t_3+ t_4$, $t_7+ t_8$ και $t_{11}+ t_{12}$. Ομοίως, και για τις μονάδες που απομένουν.

2.3 Ο μη γραμμικός μετασχηματισμός των αραιών πινάκων

Ορισμός: Γινόμενο Riesz του πίνακα U (διάστασης m x m) καλούνται οι πραγματικοί αριθμοί:

$$t_n = \prod_{k=1}^{m} \left(1 + a_k U_{k,n}\right),\ n = 1,...,m$$

όπου $a = \{a_n: n = 1,...,m\}$ είναι μία ακολουθία πραγματικών αριθμών.

Είναι εύκολο να δει κανείς ότι ο παραπάνω τύπος ορίζει έναν μη γραμμικό μετασχηματισμό:

$$\{\alpha_n: n=1,...m\} \rightarrow \{t_n: n=1,...m\}$$

ο οποίος εν γένει δεν είναι αντιστρέψιμος.

Παράδειγμα: Το Γινόμενο Riesz του πίνακα $U^4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ είναι:

$$t_1 = (1+a_1)(1+a_2)(1+a_3),\ t_2 = (1+a_1)(1+a_2),\ t_3 = (1+a_1)(1+a_4),\ t_4 = 1+a_1.$$

Σε αυτού του τύπου τα Γινόμενα Riesz, δηλαδή των πινάκων της κλάσης υπάρχει ο αντίστροφος μετασχηματισμός. Στην προκείμενη περίπτωση:

$$a_1 = t_4 - 1,\ \ a_2 = \frac{t_2}{t_4} - 1,\ \ a_3 = \frac{t_1}{t_2} - 1,\ \ a_4 = \frac{t_3}{t_4} - 1.$$

Η αντιστρεψιμότητα του μετασχηματισμού αυτού είναι χρήσιμη και μπορεί μεταξύ των άλλων να χρησιμοποιηθεί στην ανάπτυξη μίας μεθόδου κρυπτογράφησης. Δηλαδή, εάν θέλουμε να στείλουμε ένα μήνυμα **α** μέσω μίας μη ασφαλούς διόδου επικοινωνίας μπορούμε με τον μετασχηματισμό του γινομένου Riesz να το κωδικοποιήσουμε σε ένα κρυπτογραφημένο μήνυμα **t** και να το στείλουμε στο δέκτη του μηνύματος. Επειδή ο μετασχηματισμός αυτός είναι μη γραμμικός, δεν μπορεί να αποκωδικοποιηθεί εύκολα το μήνυμα από έναν εισβολέα. Επιπλέον, η χρήση των

αραιών πινάκων παρέχει τη δυνατότητα γρήγορων υπολογισμών ακόμα κι όταν η ακολουθία **α** είναι μεγάλου μήκους και αποτελείται από αριθμούς με πολλά ψηφία.

2.4 Συμπεράσματα

Οι εκπαιδευτικοί ερχόμαστε ολοένα και πιο πολύ αντιμέτωποι με ερωτήματα των μαθητών που έχουν να κάνουν με την χρήση των μαθημάτων/γνώσεων του σχολείου στην καθημερινότητά τους ή στα μελλοντικά τους επαγγέλματα. Μία επίδειξη/παρουσίαση της παρούσας εργασίας στους μαθητές της Γ΄ Λυκείου είναι δυνατό να επιφέρει θετικά αποτελέσματα σε ερωτήσεις ανάλογου περιεχομένου, καθότι η παρουσίαση των σύγχρονων ερευνητικών προβλημάτων κερδίζει το ενδιαφέρον των μαθητών, οι οποίοι μέσω του διαδικτύου και των ΜΜΕ έχουν ανάλογα ερεθίσματα. Επίσης, είναι δυνατό η παρούσα εργασία να αποτελέσει ένα μέσο ώστε το μάθημα «Ανάπτυξη Εφαρμογών σε Προγραμματιστικό Περιβάλλον» να ξεφύγει από την αυστηρότητα που πιθανώς πηγάζει από το βιβλίο. Επιπροσθέτως, αναδεικνύεται ότι η κατασκευή ενός αλγορίθμου δεν είναι μόνο η σύνταξη αυτού, ο κώδικας, αλλά είναι μία πολύπλοκη και δημιουργική διαδικασία. Συγκεκριμένα, με μεθοδικότητα και καινοτομία χρησιμοποιούνται γνώσεις του σχολείου (πίνακες) για τη δημιουργία μίας νέας θεωρίας (αραιοί πίνακες), ώστε με τη βοήθεια ενός αλγορίθμου να επιλυθεί ένα πρόβλημα (επεξεργασία της πληροφορίας). Με αυτόν τον τρόπο, γίνεται φανερό ότι μπορούν και πρέπει να συνδυάζονται οι γνώσεις/επιστήμες (διαθεματικότητα). Είναι άλλωστε κοινά αποδεκτό ότι τα μαθηματικά μοντέλα είναι χρήσιμα στην κατασκευή γρήγορων και αποτελεσματικών αλγορίθμων.

Ευχαριστίες

Η συγγραφέας του παρόντος άρθρου θα ήθελε να ευχαριστήσει τους ανώνυμους κριτές για τις εποικοδομητικές τους παρατηρήσεις και προτάσεις.

Βιβλιογραφία

Atreas, N. D., Karanikas C., & Polychronidou, P. (2008). A class of sparse unimodular matrices generating multiresolution and sampling snalysis for data of any length. *SIAM Journal on Matrix Analysis and Applications*, 30(1), 312-323.

Atreas, N. D., & Polychronidou, P. (2008), A class of sparse invertible matrices and their use for non-linear prediction of nearly periodic time series with fixed period. *Numerical Functional Analysis and Optimization*, 29(1), 66-87.

Berry, M. W., Drmac, Z., & Jessup, E. R. (1999). Matrices, vector spaces and information retrieval. *SIAM Review*, 41 (2), 335-362.

Dongarra, J. (2000), Sparse matrix storage formats in: Z. Bai et al, Templates for the Solution of Algebraic Eigenvalue problems: A Practical Guide. *SIAM,* Philadelphia, Electronic version available at: (http://www.cd.utk.edu/~dongarra/etemplates/node372.html).