Κώδικες και Λατινικά Τετράγωνα

ΧΡΗΣΤΟΣ ΖΩΧΙΟΣ

ΠΑΡΟΥΣΙΑΣΗ ΣΤΟ ΜΑΘΗΜΑ ΤΗΣ
ΚΩΔΙΚΟΠΟΙΗΣΗΣ

ΙΑΝΟΥΑΡΙΟΣ 2003

Διάλεξη που δόθηκε στις **24 Ιανουαρίου 2003** στα πλαίσια του μεταπτυχιακού μαθήματος "Κωδικοποίηση", το οποίο διδάχθηκε κατά τη διάρκεια του χειμερινού εξαμήνου 2002-2003.
Διδάσκων: Ι. Α. Αντωνιάδης.

Το κείμενο, στο μεγαλύτερο μέρος του, αποτελεί απόδοση στα ελληνικά του κεφαλαίου 10(σελ. 113 - 124) του βιβλίου Raymond Hill, **A First Course in Coding Theory**, Oxford University Press.

Περιεχόμενα

Ο βασικός στόχος αυτής της εργασίας είναι να παρουσιάσει τον τρόπο με τον οποίο κατασκευάζονται κώδικες από συγκεκριμένα σύνολα λατινικών τετραγώνων και αντιστρόφως. Πιο ειδικά, θα επιλύσουμε πλήρως "το κεντρικό πρόβλημα της θεωρίας κωδίκων", σε κάθε αλφάβητο, για κώδικες διόρθωσης ενός λάθους και μήκους 4.

1 Λατινικά τετράγωνα

Ορισμός 1 *Ένα λατινικό τετράγωνο τάξης q είναι ένας $q \times q$ πίνακας, τα στοιχεία του οποίου είναι από ένα σύνολο F_q αποτελούμενο από q διαφορετικά σύμβολα, ούτως ώστε κάθε γραμμή και κάθε στήλη του πίνακα περιέχει κάθε σύμβολο ακριβώς μία φορά.*

Παράδειγμα 1 Έστω $F_3 = \{1, 2, 3\}$. Ένα παράδειγμα λατινικού τετραγώνου τάξης 3, είναι το

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}.$$

Τα λατινικά τετράγωνα μπορούν να χρησιμοποιηθούν σε στατιστικά πειράματα.

Παράδειγμα 2 Τρία φάρμακα για τον πονοκέφαλο 1, 2, 3 πρόκειται να εξεταστούν πάνω στα αντικείμενα Α, Β, Γ τρεις διαδοχικές μέρες Δ, Τ, Τ. Ένα πιθανό πρόγραμμα είναι το

$$\begin{array}{c} \\ \text{Α} \\ \text{Β} \\ \text{Γ} \end{array} \begin{array}{c} \begin{array}{ccc} \Delta & \text{T} & \text{T} \end{array} \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \end{array}.$$

Πέρα από το να εξετάσουμε το αποτέλεσμα διαφορετικών φαρμάκων στο ίδιο αντικείμενο, θέλουμε επίσης να έχουμε κάποια μέτρηση των αποτελεσμάτων των φαρμάκων αν δοθούν σε διαφορετικές μέρες της ίδιας περιόδου των τριών ημερών. Οπότε θέλουμε κάθε φάρμακο να χρησιμοποιηθεί ακριβώς μία φορά κάθε μέρα. Απαιτούμε, δηλαδή, ένα λατινικό τετράγωνο για το πρόγραμμα, για παράδειγμα το

$$\begin{array}{c} \\ \text{Α} \\ \text{Β} \\ \text{Γ} \end{array} \begin{array}{c} \begin{array}{ccc} \Delta & \text{T} & \text{T} \end{array} \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \end{array}.$$

Θεώρημα 1 *Για κάθε θετικό ακέραιο q υπάρχει ένα λατινικό τετράγωνο τάξης q.*

Απόδειξη: Μπορούμε να θεωρήσουμε την $1\,2\,3\,\cdots\,q$ ως την πρώτη γραμμή και να την μεταθέτουμε κυκλικά μία φορά, για κάθε επικείμενη γραμμή. Έτσι παίρνουμε τον πίνακα

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & & & q \\ 2 & 3 & 4 & \cdots & & q & 1 \\ 3 & 4 & 5 & \cdots & q & 1 & 2 \\ \vdots & \vdots & \vdots & & & & \vdots \\ q & 1 & 2 & \cdots & & & q-1 \end{pmatrix}.$$

Εναλλακτικά, ο προσθετικός πίνακας του Z_q είναι ένα λατινικό τετράγωνο τάξης q. □

2 Αμοιβαίως ορθογώνια λατινικά τετράγωνα

Ορισμός 2 *Έστω A και B δύο λατινικά τετράγωνα τάξης q. Έστω a_{ij} και b_{ij} τα στοιχεία της (i,j) θέσης των A και B, αντίστοιχα. Τότε λέμε ότι οι A και B είναι αμοιβαίως ορθογώνια λατινικά τετράγωνα(συντομογραφία MOLS) αν τα q^2 διατεταγμένα ζεύγη (a_{ij}, b_{ij}), $i,j = 1,2,\ldots,q$, είναι όλα διαφορετικά.*

Με άλλα λόγια, αν υπερθέσουμε τα δύο τετράγωνα για να σχηματίσουμε ένα καινούριο $q \times q$ τετράγωνο με διατεταγμένα ζεύγη ως στοιχεία, τότε αυτά τα q^2 διατεταγμένα ζεύγη είναι όλα διαφορετικά.

Παράδειγμα 3 Τα λατινικά τετράγωνα

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix} \qquad \text{και} \qquad B = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

αποτελούν ένα ζευγάρι από MOLS τάξης 3, καθώς, αν υπερτεθούν, δίνουν τον πίνακα

$$\begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix}.$$

Εφαρμογή: Υποθέτουμε ότι τρία φάρμακα για τον πονοκέφαλο, έστω τα 1, 2, 3, και τρία φάρμακα για τον πυρετό, τα οποία συμβολιζουμε επίσης 1, 2, 3, πρόκειται να δοκιμαστούν σε τρία αντικείμενα Α, Β, Γ, τρεις διαδοχικές μέρες, έστω Δ, Τ, Τ. Όπως στο παράδειγμα 2, θα χρησιμοποιήσουμε ένα λατινικό τετράγωνο ταξης 3 για το πρόγραμμα του φαρμάκου για τον πονοκέφαλο και ένα άλλο για το πρόγραμμα του φαρμάκου για τον πυρετό. Από τη στιγμή που το κάθε αντικείμενο παίρνει ένα φάρμακο για τον πονοκέφαλο και ένα φάρμακο για τον πυρετό κάθε μέρα, έχουμε την ευκαιρία να παρατηρήσουμε το αποτέλεσμα του συνδυασμού τους. Μπορούμε να δοκιμάσουμε κάθε έναν

από τους 9 συνδυασμούς (φαρμάκου για πονοκέφαλο)/(φαρμάκου για πυρετό) ακριβώς μία φορά ; Ναι, χρησιμοποιώντας το παραπάνω ζευγάρι από MOLS.

$$\begin{array}{c} \\ \text{A} \\ \text{B} \\ \text{Γ} \end{array} \begin{array}{c} \begin{array}{ccc} \Delta & \text{T} & \text{T} \end{array} \\ \begin{pmatrix} (1,1) & (2,2) & (3,3) \\ (2,3) & (3,1) & (1,2) \\ (3,2) & (1,3) & (2,1) \end{pmatrix} \end{array}.$$

Εδώ, με (i,j) συμβολίζεται το ζευγάρι (φάρμακο πονοκέφαλου i, φάρμακο πυρετού j).

Παράδειγμα 4 Δεν υπάρχει ζευγάρι από MOLS τάξης 2, καθώς, αν $F_2 = \{1,2\}$, τότε τα μόνα λατινικά τετράγωνα τάξης 2 είναι τα $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ και $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, και αυτά δεν είναι αμοιβαίως ορθογώνια.

3 Βέλτιστοι κώδικες διόρθωσης ενός λάθους και μήκους 4

Ας θεωρήσουμε, σε ένα τυχαίο αλφάβητο F_q, "το κεντρικό πρόβλημα της θεωρίας κωδίκων" ,για κώδικες μήκους 4 και ελάχιστης απόστασης 3, δηλαδή το πρόβλημα εύρεσης της τιμής του $A_q(4,3)$. Αρχικά βρίσκουμε ένα άνω φράγμα.

Θεώρημα 2 *Ισχύει ότι* $A_q(4,3) \leq q^2$, *για κάθε* q.

Απόδειξη: Έστω C είναι ένας q-ικός $(4,M,3)$-κώδικας και $x = x_1x_2x_3x_4$, $y = y_1y_2y_3y_4$ είναι δύο διαφορετικές κωδικές λέξεις του C. Τότε $(x_1,x_2) \neq (y_1,y_2)$, γιατί αλλιώς οι x και y θα διέφεραν μόνο στις δύο τελευταίες θέσεις, κάτι που δεν μπορεί να ισχύει, αφού $d(C) = 3$. Οπότε, τα M διατεταγμένα ζεύγη που προκύπτουν παραλείποντας τις δύο τελευταίες συντεταγμένες από τον C, είναι όλα διαφορετικά διανύσματα του $(F_q)^2$, επομένως πρέπει να έχουμε $M \leq q^2$. □

Παράδειγμα 5 Για $q = 3$, το φράγμα που προκύπτει από το Θεώρημα 2, για τον κώδικα Hamming $\text{Ham}(2,3)$ είναι ένας $(4,9,3)$-κώδικας :

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 \\ 0 & 2 & 2 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 1 & 2 & 0 & 2 \\ 2 & 0 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 2 & 2 & 1 & 0 \end{pmatrix}.$$

Παρατηρούμε ότι τα διατεταγμένα ζεύγη σε κάθε δύο καθορισμένες θέσεις συντεταγμένων είναι ακριβώς τα διαφορετικά διανύσματα του $(F_3)^2$. Η παρατήρηση αυτή δικαιολογείται πλήρως από το επιχείρημα της απόδειξης του Θεωρήματος 2.

Παρατήρηση: Για $q \geq 4$, το φράγμα του Θεωρήματος 2 είναι μία μεγάλη βελτίωση του φράγματος του Hamming, το οποίο δίνει μόνο ότι $A_q(4,3) \leq q^4/(4q-3)$.

Στη συνέχεια, θα καθορίσουμε αυτές τις τιμές του q, για τις οποίες ένας q-ικός $(4, q^2, 3)$-κώδικας υπάρχει. Από τη στιγμή που τα q^2 διατεταγμένα ζεύγη που δημιουργούν οι δύο πρώτες συντεταγμένες των κωδικών λέξεων ενός τέτοιου κώδικα είναι διαφορετικά, ένας τέτοιος κώδικας πρέπει να έχει τη μορφή

$$\Big\{(i,j,a_{ij},b_{ij})|(i,j) \in (F_q)^2\Big\}.$$

Δείχνουμε, τώρα, τη σχέση που υπάρχει μεταξύ τέτοιων κωδίκων και των ζευγαριών από αμοιβαίως ορθογώνια λατινικά τετράγωνα.

Θεώρημα 3 *Υπάρχει ένας q-ικός $(4, q^2, 3)$-κώδικας αν και μόνο αν υπάρχει ένα ζευγάρι από MOLS τάξης q.*

Απόδειξη: Θα δείξουμε ότι ένας κώδικας

$$C = \Big\{(i,j,a_{ij},b_{ij})|(i,j) \in (F_q)^2\Big\}$$

είναι ένας $(4, q^2, 3)$-κώδικας αν και μόνο αν οι $A = [a_{ij}]$ και $B = [b_{ij}]$ σχηματίζουν ένα ζευγάρι από MOLS τάξης q.

Όπως στην απόδειξη του Θεωρήματος 2, η ελάχιστη απόσταση του C είναι 3 αν και μόνο αν, για κάθε ζευγάρι θέσεων των συντεταγμένων, τα διατεταγμένα ζεύγη που εμφανίζονται σε αυτές τις θέσεις είναι διαφορετικά. Τώρα, τα q^2 ζεύγη (i, a_{ij}) είναι διαφορετικά και τα q^2 ζεύγη (j, a_{ij}) είναι διαφορετικά αν και μόνο αν ο A είναι ένα λατινικό τετράγωνο. Τα q^2 ζεύγη (i, b_{ij}) είναι διαφορετικά και τα q^2 ζεύγη (j, b_{ij}) είναι διαφορετικά αν και μόνο αν ο B είναι ένα λατινικό τετράγωνο. Τελικά, τα q^2 ζεύγη (a_{ij}, b_{ij}) είναι διαφορετικά αν και μόνο αν οι A και B είναι αμοιβαίως ορθογώνιοι. □

Το Θεώρημα 3 δείχνει ότι $A_q(4,3) = q^2$ αν και μόνο αν υπάρχει ένα ζευγάρι από MOLS τάξης q. Θα δείξουμε (στο Θεώρημα 6) ότι ένα τέτοιο ζευγάρι από MOLS μπορεί να κατασκευαστεί εύκολα για τα τρία τέταρτα του συνόλου όλων των περιπτώσεων ή, πιο συγκεκριμένα, όταν ισχύει ότι $q \equiv 0, 1, \text{ή } 3 \pmod 4$.

Θεώρημα 4 *Αν ο q είναι δύναμη κάποιου πρώτου και $q \neq 2$, τότε υπάρχει κάποιο ζευγάρι από MOLS τάξης q.*

Απόδειξη: Έστω F_q το σώμα $GF(q) = \{\lambda_0, \lambda_1, \ldots, \lambda_{q-1}\}$, όπου $\lambda_0 = 0$ (αν ο q είναι πρώτος, μπορούμε να πάρουμε $\lambda_i = i$ για κάθε i). Έστω μ και ν δύο διαφορετικά, μη μηδενικά, στοιχεία του $GF(q)$. Έστω $A = [a_{ij}]$ και $B = [b_{ij}]$ δύο $q \times q$ πίνακες, που ορίζονται από τις σχέσεις

$$a_{ij} = \lambda_i + \mu\lambda_j \qquad \text{και} \qquad b_{ij} = \lambda_i + \nu\lambda_j.$$

(οι γραμμές και οι στήλες των A και B αριθμούνται ως $0, 1, \ldots, q-1$.) Αρχικά δείχνουμε ότι οι A και B είναι λατινικά τετράγωνα. Αν δύο στοιχεία στην ίδια γραμμή του A είναι παρόμοια, τότε έχουμε

$$\lambda_i + \mu\lambda_j = \lambda_i + \mu\lambda_{j'}, \quad \text{δηλαδή} \quad \mu\lambda_j = \mu\lambda_{j'},$$

από το οποίο προκύπτει ότι $j = j'$, αφού $\mu \neq 0$. Ομοίως, αν δύο στοιχεία στην ίδια στήλη του A είναι παρόμοια, τότε έχουμε

$$\lambda_i + \mu\lambda_j = \lambda_{i'} + \mu\lambda_j, \quad \text{δηλαδή} \quad \lambda_i = \lambda_{i'},$$

από το οποίο προκύπτει ότι $i = i'$. Επομένως ο A, ομοίως και ο B, είναι λατινικά τετράγωνα. Για να δείξουμε ότι οι A και B είναι ορθογώνιοι, υποθέτουμε, για άτοπο, ότι $(a_{ij}, b_{ij}) = (a_{i'j'}, b_{i'j'})$, δηλαδή υποθέτουμε ότι το ίδιο διατεταγμένο ζεύγος εμφανίζεται δύο φορές, κατά την υπέρθεση των τετραγώνων. Τότε

$$\lambda_i + \mu\lambda_j = \lambda_{i'} + \mu\lambda_{j'}$$

και

$$\lambda_i + \nu\lambda_j = \lambda_{i'} + \nu\lambda_{j'},$$

και, αφαιρώντας κατά μέλη, προκύπτει ότι

$$(\mu - \nu)\lambda_j = (\mu - \nu)\lambda_{j'}.$$

Αφού $\mu \neq \nu$, έχουμε $j = j'$ και, συμπερασματικά, $i = i'$. $\square$

Παρατήρηση: Παρατηρούμε ότι η ιδιαίτερα σημαντική ιδιότητα των σωμάτων, κατά την οποία μπορούμε να παραλείπουμε τους μη-μηδενικούς παράγοντες σε ένα γινόμενο ίσο με μηδέν, χρησιμοποιήθηκε στην παραπάνω απόδειξη. Μία παρόμοια κατασκευή χρησιμοποιώντας το Z_n, όπου n όχι πρώτος, θα αποτύγχανε να δώσει ένα ζευγάρι από MOLS.

Παράδειγμα 6 Για το $GF(3) = \{0, 1, 2\}$, η κατασκευή του Θεωρήματος 4 δίνει, παίρνοντας $\mu = 1,\ \nu = 2$:

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad \text{και} \qquad B = \begin{pmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}.$$

Ο αντίστοιχος $(4, 9, 3)$-κώδικας, που δίνεται από το Θεώρημα 3, είναι ακριβώς ο κώδικας Hamming, όπως δίνεται στο παράδειγμα 5.

Στη συνέχεια περιγράφουμε μία κατασκευή που μας δίνει ζευγάρια από MOLS τάξης q, για ακόμα πιο πολλές τιμές του q.

Θεώρημα 5 *Αν υπάρχει ένα ζευγάρι από MOLS τάξης m και υπάρχει ένα ζευγάρι από MOLS τάξης n, τότε υπάρχει ένα ζευγάρι από MOLS τάξης mn.*

Απόδειξη: Υποθέτουμε ότι A_1, A_2 είναι ένα ζευγάρι από MOLS τάξης m και B_1, B_2 είναι ένα ζευγάρι από MOLS τάξης n.

Συμβολίζουμε το (i,j)-οστό στοιχείο του A_k με $a_{ij}^{(k)} \qquad (k=1,2)$
και συμβολίζουμε το (i,j)-οστό στοιχείο του B_k με $b_{ij}^{(k)} \qquad (k=1,2)$.
Έστω C_1 και C_2 είναι δύο $mn \times mn$ τετράγωνα, ορισμένα ως εξής:

$$C_k = \begin{pmatrix} (a_{11}^{(k)}, B_k) & (a_{12}^{(k)}, B_k) & \cdots & (a_{1m}^{(k)}, B_k) \\ (a_{21}^{(k)}, B_k) & (a_{22}^{(k)}, B_k) & \cdots & (a_{2m}^{(k)}, B_k) \\ \vdots & \vdots & & \vdots \\ (a_{m1}^{(k)}, B_k) & \cdots & & (a_{mm}^{(k)}, B_k) \end{pmatrix},$$

όπου με $(a_{ij}^{(k)}, B_k)$ συμβολίζουμε έναν $n \times n$ πίνακα, του οποίου το (r,s)-οστό στοιχείο είναι το $(a_{ij}^{(k)}, b_{rs}^{(k)})$ για $r, s = 1, 2, \ldots, n$.

Με άλλα λόγια, ο C_k προκύπτει από τον A_k, αντικαθιστώντας κάθε στοιχείο a του A_k από τον $n \times n$ πίνακα (a, B_k), όπου

$$(a, B_k) = \begin{pmatrix} (a, b_{11}^{(k)}) & (a, b_{12}^{(k)}) & \cdots & (a, b_{1n}^{(k)}) \\ (a, b_{21}^{(k)}) & (a, b_{22}^{(k)}) & \cdots & (a, b_{2n}^{(k)}) \\ \vdots & \vdots & & \vdots \\ (a, b_{n1}^{(k)}) & (a, b_{n2}^{(k)}) & \cdots & (a, b_{nn}^{(k)}) \end{pmatrix}.$$

Η απόδειξη του ότι οι C_1 και C_2 είναι λατινικά τετράγωνα και ότι αυτά είναι αμοιβαίως ορθογώνια, αποτελεί απλή άσκηση. □

Παράδειγμα 7

$$\text{Οι} \quad A_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \qquad \text{και} \qquad A_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

αποτελούν ένα ζευγάρι από MOLS τάξης 3.

$$\text{Οι} \quad B_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix} \qquad \text{και} \qquad B_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

αποτελούν ένα ζευγάρι από MOLS τάξης 4.

Η κατασκευή του Θεωρήματος 5 δίνει το ακόλουθο ζευγάρι από MOLS τάξης 12, τα στοιχεία του οποίου είναι διατεταγμένα ζεύγη από το Καρτεσιανό γινόμενο $F_3 \times F_4 = \{00, 01, 02, 03, 10, 11, 12, 13, 20, 21, 22, 23\}$. (Θα μπορούσαμε να συμβολίσουμε τα στοιχεία αυτά ως τους ακέραιους $1, 2, \ldots, 12$, αν θέλαμε).

$$C_1 = \left(\begin{array}{cccc|cccc|cccc} 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 \\ 01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 & 21 & 20 & 23 & 22 \\ 02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 & 22 & 23 & 20 & 21 \\ 03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 & 23 & 22 & 21 & 20 \\ \hline 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 & 00 & 01 & 02 & 03 \\ 11 & 10 & 13 & 12 & 21 & 20 & 23 & 22 & 01 & 00 & 03 & 02 \\ 12 & 13 & 10 & 11 & 22 & 23 & 20 & 21 & 02 & 03 & 00 & 01 \\ 13 & 12 & 11 & 10 & 23 & 22 & 21 & 20 & 03 & 02 & 01 & 00 \\ \hline 20 & 21 & 22 & 23 & 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 \\ 21 & 20 & 23 & 22 & 01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 \\ 22 & 23 & 20 & 21 & 02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 \\ 23 & 22 & 21 & 20 & 03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 \end{array}\right),$$

$$C_2 = \left(\begin{array}{cccc|cccc|cccc} 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 \\ 02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 & 22 & 23 & 20 & 21 \\ 03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 & 23 & 22 & 21 & 20 \\ 01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 & 21 & 20 & 23 & 22 \\ \hline 20 & 21 & 22 & 23 & 00 & 01 & 02 & 03 & 10 & 11 & 12 & 13 \\ 22 & 23 & 20 & 21 & 02 & 03 & 00 & 01 & 12 & 13 & 10 & 11 \\ 23 & 22 & 21 & 20 & 03 & 02 & 01 & 00 & 13 & 12 & 11 & 10 \\ 21 & 20 & 23 & 22 & 01 & 00 & 03 & 02 & 11 & 10 & 13 & 12 \\ \hline 10 & 11 & 12 & 13 & 20 & 21 & 22 & 23 & 00 & 01 & 02 & 03 \\ 12 & 13 & 10 & 11 & 22 & 23 & 20 & 21 & 02 & 03 & 00 & 01 \\ 13 & 12 & 11 & 10 & 23 & 22 & 21 & 20 & 03 & 02 & 01 & 00 \\ 11 & 10 & 13 & 12 & 21 & 20 & 23 & 22 & 01 & 00 & 03 & 02 \end{array}\right).$$

Πρέπει να είναι ξεκάθαρος στον αναγνώστη ο τρόπος, σύμφωνα με τον οποίο συμπληρώθηκαν τα στοιχεία στα πιο πάνω τετράγωνα.

Η κατασκευή του Θεωρήματος 5 μπορεί να επαναληφθεί για όσες φορές θέλουμε. Για παράδειγμα, μπορούμε να πάρουμε ένα ζευγάρι από MOLS τάξης 60, παίρνοντας το ζευγάρι των MOLS τάξης 12, το οποίο κατασκευάστηκε στο παράδειγμα 7, μαζί με ένα ζευγάρι από MOLS τάξης 5, όπως αυτό δίνεται από το Θεώρημα 4. Το ακόλουθο αποτέλεσμα μας λέει ακριβώς για ποιες τιμές του q, ένα ζευγάρι από MOLS τάξης q μπορεί να κατασκευασθεί με αυτήν τη μέθοδο.

Θεώρημα 6 *Αν* $q \equiv 0, 1 \text{ ή } 3 \pmod 4$, *τότε υπάρχει ένα ζευγάρι από MOLS τάξης* q.

Απόδειξη: Υποθέτουμε ότι $q \equiv 0, 1$ ή $3 \pmod 4$. Τότε ο q είτε είναι περιττός, είτε διαιρείται με το 4. Επομένως, αν $q = p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t}$ είναι η παραγοντοποίηση του q σε δυνάμεις πρώτων, όπου $p_1, p_2, \ldots, p_t$ είναι διαφορετικοί πρώτοι και $h_1, h_2, \ldots, h_t$ είναι θετικοί ακέραιοι, τότε ισχύει ότι $p_i^{h_i} \geq 3$, για κάθε i. Άρα, από το Θεώρημα 4, υπάρχει ένα ζευγάρι από MOLS τάξης $p_i^{h_i}$, για κάθε i. Στη συνέχεια, με επαναλαμβανόμενη εφαρμογή του Θεωρήματος 5, παίρνουμε τελικά ένα ζευγάρι από MOLS τάξης $p_1^{h_1} p_2^{h_2} \cdots p_t^{h_t} = q$. □

Το Θεώρημα 6 αφήνει τις περιπτώσεις όπου $q \equiv 2 \pmod 4$, δηλαδή $q = 2, 6, 10, 14, \ldots$, ασχολίαστες. Έχει δειχθεί στο παράδειγμα 4, ότι δεν υπάρχει κάποιο ζευγάρι από MOLS τάξης 2. Ένα ζευγάρι από MOLS τάξης 6 είναι ισοδύναμο με μία λύση του "προβλήματος των 36 αξιωματικών" του Euler. Η εικασία του Euler ότι ένα τέτοιο ζευγάρι δεν υπάρχει αποδείχθηκε από τον Tarry. Ο Euler είχασε επιπλέον ότι δεν υπάρχει ένα ζευγάρι από MOLS τάξης q, για οποιοδήποτε $q \equiv 2 \pmod 4$. Για τέτοια $q \geq 10$, δεν θα μπορούσε να είχε πέσει περισσότερο έξω, αν και, μόλις το 1960 αποδείχθηκε ότι η εικασία του ήταν λαθεμένη, μέσω του παρακάτω αποτελέσματος.

Θεώρημα 7 *(Bose, Shrikhande και Parker (1960)). Υπάρχει ένα ζευγάρι από MOLS τάξης q για όλα τα q, εκτός από $q = 2$ και $q = 6$.*

Η απόδειξη του Θεωρήματος 7 για τις περιπτώσεις $q \equiv 2 \pmod 4$ είναι ιδιαίτερα περίπλοκη και παραλείπεται εδώ. □

Πόρισμα 1 *$A_q(4, 3) = q^2$ για κάθε $q \neq 2, 6$.*

Απόδειξη: Είναι άμεσο από τα Θεωρήματα 2, 3 και 7. □

Για το τέλος, θα βρούμε τις τιμές του $A_q(4, 3)$ για $q = 2$ και $q = 6$. Είναι αρκετά εύκολο το να δειχτεί ότι $A_2(4, 3) = 2$: Ο κώδικας $\{(0, 0, 0, 0), (1, 1, 1, 0)\}$ είναι ένας $(4, 2, 3)$-κώδικας στο F_2. Αν υπήρχε $(4, 3, 3)$-κώδικας τότε, για να υπάρχει ελάχιστη απόσταση ίση με 3 θα πρέπει, οι μη μηδενικές λέξεις αυτού του κώδικα να έχουν τουλάχιστον 3 άσσους και, ανά 2 οι λέξεις, να μην έχουν 2 κοινές συντεταγμένες. Όμως, οποιαδήποτε λέξη με 3 άσσους, έχει 2 κοινές συντεταγμένες με την $(1, 1, 1, 0)$. Άρα, ένας κώδικας μήκους 4 και ελάχιστης απόστασης 3 στο F_2, δεν μπορεί να έχει πάνω από 2 κωδικές λέξεις. Το παρακάτω Θεώρημα δίνει την τιμή του $A_6(4, 3)$.

Θεώρημα 8 $A_6(4, 3) = 34$.

Απόδειξη: Οι πίνακες

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 4 & 6 & 5 & 1 & 2 \\ 4 & 3 & 5 & 6 & 2 & 1 \\ 5 & 6 & 2 & 1 & 4 & 3 \\ 6 & 5 & 1 & 2 & 3 & 4 \end{pmatrix} \quad \text{και} \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 6 & 5 & 1 & 2 & 4 & 3 \\ 4 & 3 & 6 & 5 & 2 & 1 \\ 5 & 6 & 2 & 1 & 3 & 4 \end{pmatrix}$$

αποτελούν ένα ζευγάρι από λατινικά τετράγωνα, τα οποία είναι όσο το δυνατόν κοντά στο να είναι ορθογώνια. Αποτυγχάνουν μόνο στο ότι $(a_{65}, b_{65}) = (a_{13}, b_{13})$ και $(a_{66}, b_{66}) = (a_{14}, b_{14})$. Επομένως ο κώδικας

$$\Big\{(i, j, a_{ij}, b_{ij}) | (i, j) \in (F_6)^2,\ (i, j) \neq (6, 5) \text{ ή } (6, 6)\Big\}$$

είναι ένας $(4, 34, 3)$-κώδικας (απόδειξη Θεωρήματος 3).

Τώρα, αν υπήρχε ένας $(4, 35, 3)$-κώδικας C πάνω από το F_6, τότε ο C θα είχε τη μορφή

$$\Big\{(i, j, a_{ij}, b_{ij}) | (i, j) \in (F_6)^2,\ (i, j) \neq (i_0, j_0)\Big\}$$

για κάποιο (i_0, j_0). Μετά από λίγη σκέψη, ο αναγνώστης θα πρέπει να είναι ικανός να δείξει ότι οι μερικοί 6×6 πίνακες $A = [a_{ij}]$ και $B = [b_{ij}]$, από καθέναν από τους οποίους λείπει το (i_0, j_0)-οστό στοιχείο, μπορούν να συμπληρωθούν σε λατινικά τετράγωνα, τα οποία πρέπει να είναι αμοιβαίως ορθογώνια. Αυτό έρχεται σε αντίθεση με το αποτέλεσμα μη ύπαρξης του Tarry. □

Συνοψίζοντας τα αποτελέσματά μας, σχετικά με το $A_q(4, 3)$, έχουμε το

Θεώρημα 9

$$\begin{aligned} &A_q(4, 3) = q^2, \quad \textit{για όλα τα } q \neq 2, 6, \\ &A_2(4, 3) = 2, \\ &A_6(4, 3) = 34. \end{aligned}$$

Στη συνέχεια θα γενικεύσουμε κάποια από τα προηγούμενα αποτελέσματα. Αρχικά δίνουμε μία γενίκευση του φράγματος του Θεωρήματος 2, η οποία οφείλεται στον Singleton (1964).

Θεώρημα 10 *(Το φράγμα του Singleton)*

$$A_q(n, d) \leq q^{n-d+1}.$$

Απόδειξη: Υποθέτουμε ότι ο C είναι ένας q-ικός $(n, M, d)-$κώδικας. Όπως στην απόδειξη του Θεωρήματος 2, αν παραλείψουμε τις τελευταίες $d-1$ συντεταγμένες από κάθε κωδική λέξη (δηλαδή αν "κόψουμε" τον C, $d-1$ φορές), τότε τα M διανύσματα μήκους $n-d+1$ τα οποία προκύπτουν με αυτόν τον τρόπο, πρέπει να είναι διαφορετικά, άρα $M \leq q^{n-d+1}$. □

4 Σύνολα από t αμοιβαίως ορθογώνια λατινικά τετράγωνα

Ορισμός 3 *Ένα σύνολο $\{A_1, A_2, \ldots, A_t\}$ από λατινικά τετράγωνα τάξης q καλείται σύνολο αμοιβαίως ορθογωνίων λατινικών τετραγώνων (MOLS) αν κάθε ζευγάρι $\{A_i, A_j\}$ είναι ένα ζευγάρι από MOLS, για $1 \leq i < j \leq t$.*

Θεώρημα 11 *Υπάρχουν το πολύ $q-1$ λατινικά τετράγωνα σε κάθε σύνολο από MOLS τάξης q.*

Απόδειξη: Υποθέτουμε ότι $A_1, A_2, \ldots, A_t$ είναι ένα σύνολο από t MOLS τάξης q. Η ορθογωνιότητα δύο λατινικών τετραγώνων δεν παραβιάζεται αν τα στοιχεία, οποιουδήποτε τετραγώνου από αυτά, ξανασημειωθούν(ονομαστούν) με διαφορετικό τρόπο. Οπότε, μπορούμε να σημειώσουμε ξανά τα στοιχεία κάθε τετραγώνου, έτσι ώστε η πρώτη γραμμή του κάθε A_i να είναι η $12\cdots q$. Θεωρούμε, τώρα, τα t στοιχεία που εμφανίζονται στην $(2,1)$-οστή θέση των t λατινικών τετραγώνων. Κανένα από αυτά τα στοιχεία δεν μπορεί να είναι 1, αφού το 1 έχει ήδη εμφανιστεί στην πρώτη στήλη του κάθε A_i. Επίσης, δεν μπορεί δύο από αυτά τα στοιχεία να είναι ίδια, και αυτό συμβαίνει γιατί, για οποιουσδήποτε δύο από τους A_i, τα ζευγάρια $(1,1), (2,2), \ldots, (q,q)$ εμφανίζονται ήδη στην πρώτη γραμμή του αντίστοιχου υπερτεθιμένου πίνακα, ο οποίος δεν μπορεί να έχει δύο ίδια στοιχεία, καθώς προήλθε από ζευγάρι MOLS. Επομένως, πρέπει να έχουμε $t \leq q-1$. □

Ορισμός 4 *Αν υπάρχει ένα σύνολο από $q-1$ MOLS τάξης q, τότε αυτό καλείται ένα πλήρες σύνολο από MOLS τάξης q.*

Θεώρημα 12 *Αν q είναι δύναμη πρώτου, τότε υπάρχει ένα πλήρες σύνολο από $q-1$ MOLS τάξης q.*

Απόδειξη: Θεωρούμε το σώμα $GF(q) = \{\lambda_0, \lambda_1, \ldots, \lambda_{q-1}\}$ όπου το $\lambda_0 = 0$. Έστω $A_1, A_2, \ldots, A_{q-1}$ είναι $q \times q$ πίνακες, με γραμμές και στήλες που έχουν δείκτες τους $0, 1, \ldots, q-1$, στους οποίους το (i,j)-οστό στοιχείο του A_k είναι το στοιχείο του $GF(q)$, το οποίο ορίζεται ως εξής:

$$a_{ij}^{(k)} = \lambda_i + \lambda_k \lambda_j.$$

Προκύπτει, ακριβώς όπως στην απόδειξη του Θεωρήματος 4, ότι τα $A_1, A_2, \ldots, A_{q-1}$ σχηματίζουν ένα σύνολο από MOLS τάξης q. □

Παρατήρηση: Δεν είναι γνωστό εάν υπάρχει κάποιο πλήρες σύνολο από MOLS τάξης q, όταν ο q δεν είναι δύναμη κάποιου πρώτου. Απροσδόκητα, ένα πλήρες σύνολο από MOLS τάξης $q \geq 3$ είναι ισοδύναμο με ένα προβολικό επίπεδο τάξης q (βλέπε, για παράδειγμα, Ryser (1963), σελ.92, για μία απόδειξη αυτού). Άρα, μία προσέγγιση προς το να βρούμε ένα προβολικό επίπεδο τάξης

10 (το οποίο αποτελεί και την, μικρότερης τάξης, άλυτη περίπτωση), είναι το να ψάξουμε να βρούμε ένα σύνολο από 9 MOLS τάξης 10. Παρ'όλ'αυτά, κανένας δεν έχει καταφέρει ακόμα να βρει, ακόμα και ένα σύνολο από 3 MOLS τάξης 10.

Θεώρημα 13 *Ένας $q-$ικός $(n, q^2, n-1)-$κώδικας είναι ισοδύναμος με ένα σύνολο από $n-2$ MOLS τάξης q.*

Απόδειξη: Όπως στο Θεώρημα 3, ένας $(n, q^2, n-1)-$κώδικας C πάνω από το σώμα F_q, έχει τη μορφή

$$\left\{(i, j, a_{ij}^{(1)}, a_{ij}^{(2)}, \ldots, a_{ij}^{(n-2)}) | (i,j) \in (F_q)^2\right\}.$$

Είναι πολύ απλό να δειχτεί ότι $d(C) = n-1$ αν και μόνο αν τα $A_1, A_2, \ldots, A_{n-2}$, όπου $A_k = [a_{ij}^{(k)}]$, σχηματίζουν ένα σύνολο από MOLS τάξης q. Η διαδικασία είναι ακριβώς παρόμοια με αυτήν της απόδειξης του Θεωρήματος 3. □

Πόρισμα 2 *$A_q(3,2) = q^2$, για όλα τα q.*

Απόδειξη: Ένας $(3, q^2, 2)-$κώδικας είναι ισοδύναμος με ένα μονό λατινικό τετράγωνο τάξης q, το οποίο υπάρχει, λόγω του Θεωρήματος 1. Το φράγμα του Singleton δείχνει ότι ένας τέτοιος κώδικας είναι βέλτιστος. □

Πόρισμα 3 *Αν ο q είναι δύναμη κάποιου πρώτου και $n \leq q+1$, τότε*

$$A_q(n, n-1) = q^2.$$

Απόδειξη: Αυτό είναι άμεσο από τα Θεωρήματα 10, 12 και 13. □

Για άλλους τρόπους με τους οποίους συνδέονται τα λατινικά τετράγωνα και οι κώδικες διόρθωσης λαθών, βλέπε Dénes και Keedwell (1974).

Αναφορές

[1] Bose, R. C., Shrikhande, S. S., and Parker, E. T. (1960). Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canad. J. Math.* **12**, 189-203.

[2] Dénes, J. and Keedwell, A. D. (1974). *Latin squares and their applications*. Academic Press, New York.

[3] Golomb, S. W. and Posner, E. C. (1964). Rook domains, Latin squares, affine planes, and error-distribution codes. *IEEE Trans. Info. Theory* **10**, 196-208.

[4] Ryser, H. J. (1963). *Combinatorial mathematics*. Carus Monograph 14, Math. Assoc. America.

[5] Singleton, R. C. (1964). Maximum distance q-nary codes. *IEEE Trans. Info. Theory* **10**, 116-118.

[6] Stinson, D. R. (1984). A short proof of the nonexistence of a pair of orthogonal Latin squares of order six. *J. Comb. Theory*, Ser. A **36**, 373-376.

[7] Tarry, G. (1901). Le probléme des 36 officiers. *C. R. Acad. Sci. Paris* **2**, 170-203.