• Σχεδιασμοί και κώδικες.

Ορ.: Ένας σχεδιασμός αποτελείται από γνήσια υποσύνολα (blocks) ενός συνόλου στοιχείων (varieties ή ποικιλίες), όπου:
(i) κάθε υποσύνολο (block) έχει τον ίδιο αριθμό στοιχείων
και (ii) κάθε ζεύγος στοιχείων (ποικιλιών) ανήκει στον ίδιο αριθμό υποσυνόλων (blocks)

Παράδειγμα: $K=\{1,2,3,4,5,6,7,8,9\}$

$\{1,2,3\}$, $\{4,5,6\}$, $\{7,8,9\}$, $\{1,4,7\}$, $\{1,5,9\}$, $\{2,5,8\}$

$\{3,6,9\}$, $\{2,6,7\}$, $\{3,4,8\}$, $\{1,6,8\}$, $\{2,4,9\}$, $\{3,5,7\}$.

Θεώρημα 1: Έστω σχεδιασμός με v ποικιλίες και b blocks όπου κάθε block περιέχει k ποικιλίες και όπου κάθε ζεύγος ποικιλιών περιέχεται σε λ blocks. Τότε κάθε ποικιλία περιέχεται ακριβώς σε r blocks, όπου $r=\frac{bk}{v}=\frac{\lambda(v-1)}{k-1}$.

Απόδειξη: Έστω x μια οποιαδήποτε ποικιλία του σχεδιασμού και έστω ότι αυτή ανήκει σε r_x blocks. Θεωρούμε το σύνολο των ζευγών ποικιλιών, στα οποία το ένα στοιχείο είναι το x. Αθροίζουμε τον αριθμό των συμμετοχών αυτών των ζευγών στα blocks (με δύο διαφορετικούς τρόπους). Σε κάθε block που ανήκει το x υπάρχουν $k-1$ τέτοια ζεύγη, ενώ το x ανήκει συνολικά σε r_x blocks. Επομένως ο αριθμός συμμετοχών αυτών των ζευγών

στα blocks ισούται με $r_x(k-1)$.
Επίσης ο αριθμός των ζευγών αυτών ισούται με $v-1$ και κάθε τέτοιο ζεύγος ανήκει σε λ blocks. Άρα ο αριθμός των συμμετοχών αυτών των ζευγών ισούται με $\lambda(v-1)$.
Επομένως

$$r_x(k-1)=\lambda(v-1),$$

και άρα $r=\dfrac{\lambda(v-1)}{k-1}$.

Για να αποδείξουμε ότι $r=\dfrac{bk}{v}$ εργαζόμαστε ως εξής: Αθροίζουμε τον αριθμό των συμμετοχών των ποικιλιών στα blocks.
Κάθε ποικιλία συμμετέχει σε r blocks (υπάρχουν v ποικιλίες). Επίσης κάθε block περιέχει k ποικιλίες (υπάρχουν b blocks).
Άρα

$$v.r=b.k \Rightarrow r=\frac{bk}{v}.$$

Χρησιμοποιώντας και το προηγούμενο θεώρημα, βλέπουμε ότι σε κάθε σχεδιασμό αντιστοιχούν οι εξής πέντε παράμετροι.

v: αριθμός ποικιλιών
b: αριθμός των blocks, k: αριθμός ποικιλιών σε κάθε block, r: αριθμός των blocks, στα οποία ανήκει μια ποικιλία.
λ: αριθμός των blocks, στα οποία ανήκει ένα ζεύγος ποικιλιών.

Ένας τέτοιος σχεδιασμός ονομάζεται (v,b,r,k,λ)-σχεδιασμός.

Παρατήρηση: Εάν μας δοθούν μόνον οι 3 παράμετροι ενός σχεδιασμού, εμείς μπορούμε να προσδιορίσουμε τις άλλες 2.

Σημείωση: Εάν μας δοθούν 5 αριθμοί οι οποίοι ικανοποιούν τις σχέσεις του προηγούμενου θεωρήματος, δεν σημαίνει απαραίτητα ότι υπάρχει σχεδιασμός μ' αυτούς ως παραμέτρους.

Πίνακες σχεδιασμών.

Ορ. Έστω σύνολο $\{x_1, x_2, \ldots, x_v\}$ και $(A_1, A_2, \ldots, A_b)$ οικογένεια υποσυνόλων του. Θεωρούμε πίνακα $M = [m_{ij}]$ μεγέθους $b \times v$, ο οποίος ορίζεται ως εξής:

$$m_{ij} = \begin{cases} 1 & \text{εάν } x_j \in A_i \\ 0 & \text{εάν } x_j \notin A_i \end{cases}$$

Εάν η οικογένεια υποσυνόλων αποτελεί σχεδιασμό, τότε ο πίνακας M, ονομάζεται πίνακας πρόσπτωσης αυτού του σχεδιασμού.

Παράδειγμα: Ο πίνακας πρόσπτωσης του σχεδιασμού της σελίδας 31 θα είναι ένας πίνακας μεγέθους 12×9 και θα είναι ο εξής:

$$
M = \begin{array}{c} \\ \left[\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}\right. \end{array}
$$

$$
\begin{array}{ccccccccc|l}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \\
\hline
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & \{1,2,3\} \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & \{4,5,6\} \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & \{7,8,9\} \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & \{1,4,7\} \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & \{1,5,9\} \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & \{2,5,8\} \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & \{3,6,9\} \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & \{2,6,7\} \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & \{3,4,8\} \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \{1,6,8\} \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & \{2,4,9\} \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & \{3,5,7\}
\end{array}
$$

Παρατηρήσεις: Ο πίνακας πρόσπτωσης ενός σχεδιασμού έχει τις εξής ιδιότητες:

α) Σε κάθε γραμμή υπάρχουν k 1.

β) Σε κάθε στήλη υπάρχουν r 1

γ) Για κάθε ζεύγος στηλών, υπάρχουν ακριβώς λ θέσεις, στις οποίες και οι δύο στήλες εμφανίζουν τον αριθμό 1.

Θεώρημα 2: Έστω οικογένεια b υποσυνόλων ενός συνόλου v στοιχείων και έστω ότι κάθε υποσύνολο περιέχει ακριβώς k στοιχεία ($1<k<v$). Γι' αυτή την οικογένεια συνόλων κατασκευάζουμε έναν πίνακα M, όπως αυτόν που ορίσαμε στη σελ.33.

Ο πίνακας M είναι ο πίνακας πρόσπτωσης ενός (v,b,r,k,λ)-σχεδιασμού εάν και μόνον εάν ο πίνακας $M^T.M$ είναι ο πίνακας

$$\begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & & \ddots & \vdots \\ & & & \lambda \\ \lambda & \lambda & \cdots \lambda & r \end{bmatrix}$$

μεγέθους $v \times v$

Επίσης $|M^T.M| = (r+(v-1)\lambda)(r-\lambda)^{v-1} > 0.$

Απόδειξη: Έχουμε ότι: εάν $M^T.M = [a_{ij}]$,

$a_{ij} =$ (i-γραμμή του M^T). (j-στήλη του M) =

= (i-στήλη του M). (j-στήλη του M) =

= εάν $i=j \rightarrow$ αριθμός των 1 στην i-στήλη του M

εάν $i \neq j \rightarrow$ αριθμός θέσεων στις οποίες τόσο η στήλη i, όσο και η στήλη j εμφανίζουν το 1.

Ο πίνακας M είναι ο πίνακας πρόσπτωσης ενός (v, b, r, k, λ)-σχεδιασμού $\Leftrightarrow$

$a_{ij} = r$ όταν $i = j$

$a_{ij} = \lambda$ όταν $i \neq j$

Στην συνέχεια θα αποδείξουμε ότι:

$$|M^T M| = (r+(v-1)\lambda)(r-\lambda)^{v-1}$$

Έχουμε

$$\begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \lambda & \cdots & r \end{bmatrix} \sim \begin{bmatrix} r+(v-1)\lambda & (v-1)\lambda+r & \cdots & (v-1)\lambda+r \\ \lambda & r & \cdots & \lambda \\ \vdots & & & \vdots \\ \lambda & \lambda & \cdots & r \end{bmatrix} \sim$$

$$\begin{bmatrix} r+(v-1)\lambda & 0 & 0 & \cdots & 0 \\ \lambda & r-\lambda & 0 & \cdots & 0 \\ \lambda & 0 & r-\lambda & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda & 0 & 0 & \cdots & r-\lambda \end{bmatrix}$$

Επειδή ο παραπάνω πίνακας είναι τριγωνικός η ορίζουσά του θα ισούται με $(r+(v-1)\lambda)\cdot(r-\lambda)^{v-1}$.

Για να αποδείξουμε ότι η παραπάνω ορίζουσα είναι θετική, αρκεί να αποδείξουμε ότι $r>\lambda$. Όμως και τέτοιο ισχύει διότι $r=\dfrac{\lambda(v-1)}{k-1}$ όπου

$1<k<v$.

Θεώρημα 3 (Fisher, 1940). Για κάθε (v,b,r,k,λ)-σχεδιασμό έχουμε ότι $b \geq v$.

Απόδειξη: Έστω ότι υπάρχει (v,b,r,k,λ)-σχεδιασμός με $v>b$ και έστω M, ο πίνακας πρόσπτωσης ενός τέτοιου σχεδιασμού. Ο πίνακας M θα είναι ένας πίνακας μεγέθους $b\times v$ (με περισσότερες στήλες απ' ότι γραμμές). Προσθέτουμε στον M $v-b$ μηδενικές γραμμές, οπότε "παίρνουμε" ένα πίνακα $N := \begin{pmatrix} M \\ 0 \end{pmatrix}$ μεγέθους $v\times v$.

Οπότε έχουμε

$$N^T \cdot N = \begin{pmatrix} M \\ 0 \end{pmatrix}^T \cdot \begin{pmatrix} M \\ 0 \end{pmatrix} = \begin{pmatrix} M^T & 0 \end{pmatrix} \cdot \begin{pmatrix} M \\ 0 \end{pmatrix} = M^T \cdot M$$

(

$$\underset{b\times v}{M} = [m_{ij}] = \begin{bmatrix} m_{11} & m_{12} & \cdots & m_{1v} \\ \vdots & & & \vdots \\ m_{b1} & m_{b2} & \cdots & m_{bv} \end{bmatrix}$$

$$(M^T\, 0)\begin{pmatrix} M \\ 0 \end{pmatrix} = \underset{v\times v}{\begin{bmatrix} m_{11} & \cdots & m_{b1} & 0 & \cdots & 0 \\ \vdots & & \vdots & & & \\ m_{1v} & \cdots & m_{bv} & 0 & \cdots & 0 \end{bmatrix}} \underset{v\times v}{\begin{bmatrix} m_{11} & \cdots & m_{1v} \\ \vdots & & \vdots \\ m_{b1} & \cdots & m_{bv} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{bmatrix}} =$$

$$= \underset{v\times b}{M^T} \cdot \underset{b\times v}{M} \;)$$

Όμως όπως είδαμε προηγούμενα ο $M^T.M$ έχει θετική ορίζουσα.
Άρα

$$|N|^2 = |N|.|N| = |N^T|.|N| = |N^T.N| = |M^T.M| > 0, \quad \llcorner \text{ΑΤΟΠΟ}$$

διότι ο πίνακας N έχει μηδενικές γραμμές και επομένως $|N| = 0$

Παρατήρηση: Από το προηγούμενο θεώρημα προκύπτει ότι ο μέγιστος αριθμός ποικιλιών που μπορούμε να έχουμε σ' ένα σχεδιασμό ισούται με τον αριθμό των blocks, και επειδή $r = \frac{bk}{v}$ θα έχουμε $r = k$. Σ' αυτή την περίπτωση δηλαδή θα πρόκειται για ένα (v,v,k,k,λ)-σχεδιασμό. Σχεδιασμούς με αυτά τα χαρακτηριστικά τους ονομάζουμε ΣΥΜΜΕΤΡΙΚΟΥΣ.

Στην συνέχεια θ' αναφερθούμε σε μια ειδική κατηγορία συμμετρικών σχεδιασμών, τους κυκλικούς σχεδιασμούς.

Ορισμός: Ένα υποσύνολο P του $\{0,1,2,\ldots,v-1\}$ θα ονομάζεται σύνολο τέλειας διαφοράς modv, εάν στον πίνακα διαφοράς modulo v του P κάθε στοιχείο του $\{1,2,\ldots,v-1\}$ εμφανίζεται τον ίδιο αριθμό φορών.

Παράδειγμα:

$\{0,1,2,\dots,10\}$ δηλαδή $v=11$.
$P=\{1,3,4,5,9\}$

$-(\mathrm{mod}\,11)$	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	5
4	3	1	0	10	6
5	4	2	1	0	7
9	8	6	5	4	0

Το P είναι σύνολο τέλειας διαφοράς mod 11.

Θεώρημα 4: Έστω $B_0=\{b_1,b_2,\dots,b_k\}$ υποσύνολο του $\{0,1,2,\dots,v-1\}$ με $1<k<v$. Για κάθε $0\leq i\leq v-1$, ορίζουμε σύνολα $B_i=\{b_1+i,\dots,b_k+i\}$.
Τότε τα σύνολα $B_0,B_1,\dots,B_{v-1}$ ορίζουν ένα σχεδιασμό εάν και μόνον εάν το B_0 είναι σύνολο τέλειας διαφοράς mod v.
(Και εδώ η πρόσθεση θεωρείται modulo v)

Απόδειξη: Τα σύνολα $B_0,B_1,\dots,B_{v-1}$ έχουν τον ίδιο αριθμό στοιχείων (k τον αριθμό).
Άρα για να αποδείξουμε ότι αποτελούν

σχεδιασμό αρκεί να αποδείξουμε ότι κάθε ζεύγος στοιχείων του $\{0,1,2,\dots,v-1\}$ ανήκει στον ίδιο αριθμό υποσυνόλων $B_0, B_1, \dots, B_{v-1}$.
Εμείς αρχικά θα πάρουμε δύο στοιχεία του $\{0,1,2,\dots,v-1\}$, το 0 και το j, και θα εξετάσουμε κάτω από ποιές προϋποθέσεις ανήκουν σ' ένα σύνολο B_i.
Ας υποθέσουμε εδώ, χωρίς να βλάψουμε την γενικότητα των επιχειρημάτων μας, ότι $0 \notin B_0$.
Έστω ότι

$$B_i = \{b_1+i, \dots, b_\alpha+i, \dots, b_\beta+i, \dots, b_k+i\}.$$

Θα εξετάσουμε κάτω από ποιές συνθήκες
$b_\alpha+i=0$ και $b_\beta+i=j$.
Έστω ότι ισχύει το παραπάνω. Τότε αυτό σημαίνει ότι $b_\alpha+i=v$ και $b_\beta+i\equiv j \pmod{v}$.
Δηλαδή $i=v-b_\alpha$ και $b_\beta+i=mv+j \Rightarrow b_\beta+v-b_\alpha=$

$$=mv+j \Rightarrow j=b_\beta-b_\alpha+(-m+1)v.$$

Επομένως όταν $0,j\in B_i$, $v-b_\alpha=i$ και
$j=(b_\beta-b_\alpha)(\mathrm{mod}\, v)$.

Αντίστροφα έστω ότι $i=v-b_\alpha$ και
$j=(b_\beta-b_\alpha)(\mathrm{mod}\, v)$. Τότε

$$i=v-b_\alpha \quad \text{και} \quad b_\beta+i=b_\beta-b_\alpha+b_\alpha+i=b_\beta-b_\alpha+v,$$

δηλαδή $b_\beta+i\equiv j \pmod{v}$.

Άρα $0, j \in B_i$ εάν και μόνον εάν

$i = v - b_\alpha$ και $j \equiv (b_\beta - b_\alpha)(\mathrm{mod}\, v)$.

Επομένως κάθε φορά που $j \equiv (b_\beta - b_\alpha)(\mathrm{mod}\, v)$, $0, j \in B_{v - b_\alpha}$ και αντίστροφα.

Άρα υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των φορών που το 0 και το j συνυπάρχουν σ' ένα εκ των συνόλων $B_0, B_1, \ldots$ $\ldots, B_{v-1}$ και των φορών που δύο στοιχεία του B_0 διαφέρουν κατά $j\,(\mathrm{mod}\, v)$

Όμως ο αριθμός των φορών που δύο στοιχεία του B_0 διαφέρουν κατά $j\,(\mathrm{mod}\, v)$ ισούται με τον αριθμό των εμφανίσεων του στοιχείου j στον πίνακα διαφοράς modulo v του B_0

Επομένως ο αριθμός των φορών που το ζεύγος $\{0, j\}$ ανήκει σε κάποιο σύνολο ισούται με τον αριθμό των εμφανίσεων του j στον πίνακα διαφοράς modulo v του B_0.

Τώρα η κυκλική φύση των συνόλων συνεπάγεται ότι το ζεύγος $\{0, 3\}$ εμφανίζεται αριθμό φορών ίσο με το ζεύγος $\{1, 4\}$ ή $\{2, 5\}$ κ.τ.λ.π.

Άρα κάθε ζεύγος στοιχείων θα ανήκουν στον ίδιο αριθμό συνόλων εάν και μόνον εάν κάθε αριθμός j $(1 \leq j < v)$ εμφανίζεται τον ίδιο αριθμό φορών στο πίνακα διαφοράς modulo v του B_0 δηλαδή εάν και μόνον εάν το B_0 είναι σύνολο τέλειας διαφοράς mod v

Σημείωση: Όπως αναφέραμε και προηγουμένως οι συμμετρικοί σχεδιασμοί στους οποίους αναφέρεται το Θεώρημα 4 ονομάζονται κυκλικοί.

Χρησιμοποιώντας το Θεώρημα 4 και ξεκινώντας από ένα σύνολο τέλειας διαφοράς mod v μπορούμε να κατασκευάσουμε έναν κυκλικό σχεδιασμό. Βέβαια για να είναι χρήσιμο το παραπάνω Θεώρημα χρειαζόμαστε ένα συστηματικό τρόπο εύρεσης τέτοιων συνόλων. Ένα τέτοιο Θεώρημα είναι το ακόλουθο.

Θεώρημα 5: Έστω v πρώτος αριθμός της μορφής $4n-1$ για κάποιο ακέραιο n. Έστω επίσης ότι οι δυνάμεις ενός αριθμού θ modulo v μας δίνουν το σύνολο $\{1,2,\ldots,v-1\}$. δηλαδή $\{\theta,\theta^2,\ldots,\theta^{v-1}\}=\{1,2,\ldots,v-1\}$. Τότε το σύνολο $\{\theta^2,\theta^4,\ldots,\theta^{v-1}\}$, θα είναι σύνολο τέλειας διαφοράς mod v

Απόδειξη: Παραλείπεται.

Παρατήρηση: Ξεκινώντας από ένα τέτοιο σύνολο τέλειας διαφοράς mod v μπορούμε να κατασκευάσουμε τον κυκλικό σχεδιασμό $(4n-1,4n-1,2n-1,2n-1,n-1)$.

Παράδειγμα: Θεωρούμε το σύνολο $\{0,1,2,\ldots,9,10\}$. Εδώ έχουμε $v=11=4n-1$, δηλαδή $n=3$. Θέλουμε να κατασκευάσουμε ένα κυκλικό $(11,11,5,5,2)$ - σχεδιασμό

Υπάρχει θ έτσι ώστε $\{\theta,\theta^2,\theta^3,\ldots,\theta^{10}\}=$

$=\{1,2,3,\ldots,10\}$ (Εδώ οι δυνάμεις του θ θεωρούνται modν δηλαδή mod11)

Πράγματι εάν $\theta=2$,

$$\theta^1=2^1=2$$
$$\theta^2=2^2=4$$
$$\theta^3=2^3=8$$
$$\theta^4=2^4=16\equiv 5$$
$$\theta^5=2^5=32\equiv 10$$
$$\theta^6=2^6=64\equiv 9$$
$$\theta^7=2^7=128\equiv 7$$
$$\theta^8=2^8=256\equiv 3$$
$$\theta^9=2^9=512\equiv 6$$
$$\theta^{10}=2^{10}=1024\equiv 1$$

Βάσει του Θεωρήματος 5 το σύνολο

$\{\theta^2,\theta^4,\ldots,\theta^{v-1}\}=\{4,5,9,3,1\}$ είναι σύνολο

τέλειας διαφοράς mod11.

Ας το επαληθεύσουμε:

$-\bmod 11$	1	3	4	5	9
1	0	9	8	7	3
3	2	0	10	9	5
4	3	1	0	10	6
5	4	2	1	0	7
9	8	6	5	4	0

Κάθε στοιχείο του $\{1,2,\dots,10\}$ εμφανίζεται στον πίνακα 2 φορές

Στην συνέχεια ξεκινώντας από το $\{1,3,4,5,9\}$ και χρησιμοποιώντας το Θεώρημα 4, θα κατασκευάσουμε έναν συμμετρικό κυκλικό σχεδιασμό. Θέτουμε

$$B_0=\{1,3,4,5,9\}$$
$$B_1=\{1+1,3+1,4+1,5+1,9+1\}=\{2,4,5,6,10\}$$
$$B_2=\{2+1,4+1,5+1,6+1,10+1\}=\{3,5,6,7,0\}$$
$$B_3=\{3+1,5+1,6+1,7+1,0+1\}=\{4,6,7,8,1\}$$
$$B_4=\{4+1,6+1,7+1,8+1,1+1\}=\{5,7,8,9,2\}$$
$$B_5=\{5+1,7+1,8+1,9+1,2+1\}=\{6,8,9,10,3\}$$
$$B_6=\{7,9,10,0,4\}$$
$$B_7=\{8,10,0,1,5\}$$
$$B_8=\{9,0,1,2,6\}$$
$B_9=\{10,1,2,3,7\}$ και $B_{10}=\{0,2,3,4,8\}$

Εδώ έχουμε κατασκευάσει ένα κυκλικό $(11, 11, 5, 5, 2)$-σχεδιασμό διότι $v=b=11$, $k=r=5$ και $\lambda=2$ (όσες φορές κάθε μη-μηδενικό στοιχείο εμφανίζεται στον πίνακα διαφοράς modulo v του αρχικού συνόλου $B_0=\{1,3,4,5,9\}$.)

Οι συμμετρικοί σχεδιασμοί έχουν και την εξής ενδιαφέρουσα ιδιότητα.

Θεώρημα 6: Εάν M είναι ο πίνακας πρόσπτωσης ενός συμμετρικού σχεδιασμού, τότε και ο M^T είναι επίσης πίνακας πρόσπτωσης ενός συμμετρικού σχεδιασμού. (Ο σχεδιασμός αυτός ονομάζεται δυϊκός του αρχικού).

Απόδειξη: Έστω M, ο πίνακας πρόσπτωσης ενός (v, v, k, k, λ)-σχεδιασμού (Ο σχεδιασμός αυτός θα είναι προφανώς συμμετρικός). Ο πίνακας M θα είναι μεγέθους $v \times v$, θα έχει για στοιχεία του, τα 0 και 1 σε κάθε γραμμή θα υπάρχουν k στοιχεία που είναι ίσα με 1 και σε κάθε στήλη επίσης k στοιχεία που είναι 1.

Από το Θεώρημα 2, έχουμε ότι

$$M^T . M = \begin{bmatrix} k & \lambda & \cdots & \lambda \\ \lambda & k & \cdots & \lambda \\ \vdots & \vdots & \ddots & \vdots \\ \lambda & \lambda & \cdots & k \end{bmatrix} = \Lambda + (k-\lambda) I$$

όπου Λ πίνακας μεγέθους $v \times v$, του οποίου

όλα τα στοιχεία είναι λ.
Ο πίνακας M^T θα είναι μεγέθους $v \times v$ και θα έχει k στοιχεία που είναι ίσα με 1 σε κάθε γραμμή.
Βάσει του Θεωρήματος 2, ο M^T θα είναι ο πίνακας πρόσπτωσης ενός (v,v,k,k,λ)-σχεδιασμού εάν και μόνον εάν

$(M^T)^T \cdot M^T = \Lambda + (k-\lambda)I$. Με άλλα λόγια αρκεί να αποδείξουμε ότι

$$M^T \cdot M = MM^T$$

Από το Θεώρημα 2, επίσης έχουμε

$|M^T \cdot M| > 0$ και επομένως

$$|M|^2 = |M||M| = |M^T| \cdot |M| = |M^T \cdot M| > 0$$

Άρα $|M| \neq 0$ και επομένως ο <u>M είναι αντιστρέψιμος</u>.
Τώρα

$$\underline{M\Lambda} = \begin{bmatrix} k\lambda & k\lambda & \cdots & k\lambda \\ \vdots & & & \\ k\lambda & k\lambda & \cdots & k\lambda \end{bmatrix} = \underline{\Lambda M}$$

Οπότε έχουμε,

$$\begin{aligned} MM^T &= (M \cdot M^T)(MM^{-1}) \\ &= M(M^T \cdot M)M^{-1} \end{aligned}$$

$$
\begin{aligned}
MM^T &= M(\Lambda+(k-\lambda)I)M^{-1}\\
&= M\Lambda M^{-1}+(k-\lambda)MIM^{-1}\\
&= \Lambda MM^{-1}+(k-\lambda)I\\
&= \Lambda+(k-\lambda)I\\
&= M^T\cdot M
\end{aligned}
$$

Άρα ο M^T είναι ο πίνακας πρόσπτωσης ενός (v,v,k,k,λ)-σχεδιασμού.

Από το Θεώρημα 6, προκύπτουν τα εξής πορίσματα:

Πόρισμα 1: Σε κάθε ζεύγος γραμμών του πίνακα πρόσπτωσης ενός Ω (v,v,k,k,λ)-σχεδιασμού υπάρχει ταύτιση στοιχείων που είναι 1, σε ακριβώς λ θέσεις.

Απόδειξη: Έστω M ο πίνακας πρόσπτωσης ενός τέλειου σχεδιασμού. Βάσει του Θεωρήματος 6, ο πίνακας M^T αποτελεί επίσης τον πίνακα πρόσπτωσης ενός (v,v,k,k,λ)-σχεδιασμού. Τώρα εάν πάρουμε δύο οποιεσδήποτε στήλες του M^T, θα έχουμε ταύτιση στοιχείων που είναι 1 σε ακριβώς λ θέσεις (ο αριθμός αυτός αντιπροσωπεύει το πλήθος των blocks, στα οποία ανήκουν ταυτόχρονα οι δύο ποικιλίες που αντιστοιχούν στις δύο στήλες)

Τώρα οι στήλες του M^T αποτελούν τις γραμμές του M, οπότε προκύπτει το παραπάνω Πόρισμα.

Πόρισμα 2: Κάθε ζεύγος γραμμών του πίνακα πρόσπτωσης ενός (v,v,k,k,λ)-σχεδιασμού διαφέρουν ακριβώς σε $2(k-\lambda)$-θέσεις.

Απόδειξη:
Η εικόνα που θα παρουσιάζουν οι δύο γραμμές, θα είναι η εξής:

$$\begin{array}{c|c|c|c}
 & \multicolumn{2}{c}{\overbrace{\hspace{12em}}^{k}} & \\
0\;0\ldots0 & 1\;1\ldots1 & 1\;1\ldots1 & 0\;0\ldots0 \\
1\;1\ldots1 & 1\;1\ldots1 & 0\;0\ldots0 & 0\;0\ldots0 \\
\underbrace{\hspace{5em}}_{k-\lambda} & \underbrace{\hspace{5em}}_{\lambda} & \underbrace{\hspace{5em}}_{k-\lambda} & \\
\multicolumn{2}{c}{\underbrace{\hspace{12em}}_{k}} & &
\end{array}$$

ΘΕΩΡΙΑ ΚΩΔΙΚΩΝ.

Θα ασχοληθούμε μόνον με δυαδικούς κώδικες των οποίων όλες οι κωδικές λέξεις έχουν το ίδιο μήκος.

(Δυαδικό-κώδικα ονομάζουμε κάθε σύνολο 0-1 ακολουθιών.
Τα στοιχεία αυτού του συνόλου ονομάζονται κωδικές-λέξεις).

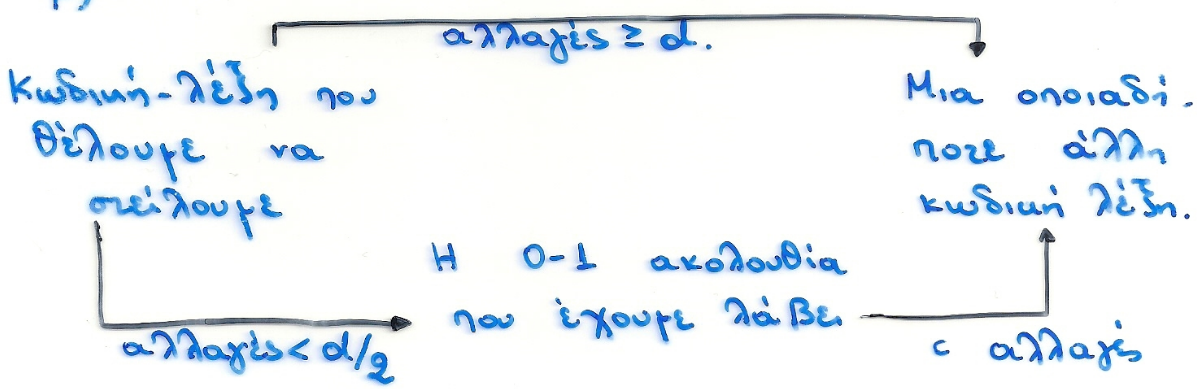
Θεώρημα: Έστω κώδικας του οποίου οι κωδικές-λέξεις έχουν την εξής ιδιότητα: Μπορούμε να "πάμε" από την μία στην άλλη με τουλάχιστον d αλλαγές.

α) εάν στην μετάδοση μιας κωδικής-λέξης ο αριθμός των λανθασμένων ψηφίων είναι μικρότερος του d, τότε μπορεί να εντοπισθεί η λανθασμένη μετάδοση, και

β) η λανθασμένη μετάδοση μιας κωδικής-λέξης μπορεί να διορθωθεί εάν ο αριθμός των λανθασμένων ψηφίων είναι μικρότερος του $\frac{1}{2}d$.

<u>Απόδειξη</u>: α) Προφανές διότι εάν συμβεί κάποιο λάθος στην μετάδοση, η κωδική-λέξη που θα προκύψει δεν θα ανήκει στο σύνολο των κωδικών-λέξεων του κώδικα.

β)



Για να πάμε από την κωδική-λέξη που θέλουμε να στείλουμε σε μια άλλη οποιαδήποτε κωδική-λέξη χρειαζόμαστε λιγότερες από $\frac{d}{2}+c$ αλλαγές. Επομένως

$$\frac{1}{2}d + c > d$$

Άρα

$$c > \frac{d}{2}.$$

Επομένως η κωδική-λέξη που θέλουμε να στείλουμε είναι η μόνη, από τις κωδικές-λέξεις, που μπορεί να προκύψει από την 0-1 ακολουθία που έχουμε λάβει, με λιγότερες από $\frac{d}{2}$ αλλαγές.

Πόρισμα: Έστω ότι οι κωδικές-λέξεις ενός κώδικα αποτελούνται από τις γραμμές του πίνακα πρόσπτωσης ενός (v,v,k,k,λ)-σχεδιασμού. Τότε

(α) στον κώδικα αυτό εντοπίζουμε λανθασμένη μετάδοση μιας κωδικής λέξης, εάν ο αριθμός των λαθών είναι μικρότερος του $2(k-\lambda)$.

(β) μια λανθασμένη μετάδοση κωδικής-λέξης μπορεί να διορθωθεί εάν ο αριθμός των λανθασμένων ψηφίων είναι μικρότερος του $(k-\lambda)$.