Natural Science Report. Ochanomizu University, Vol. 42, No. 1, 1991 13
お茶の水女子大学 自然科学報告 第42巻 第1号

On Applications of the Bruck-Ryser-Chowla Theorem

Toshiko Koyama

Department of Information Sciences, Faculty of Science,
Ochanomizu University, Tokyo

(Received April 10, 1991)

The Bruck-Ryser-Chowla theorem gave necessary conditions for the existence of symmetric designs (cf. [1] and [3]). We generalized this theorem to some family of square matrices with rational entries and applied it to the adjacency matrices of some strongly regular graphs.

THEOREM 1. *Let I denote the $n\times n$ identity matrix and J the $n\times n$ matrix each entry of which is* 1. *If n is odd and an $n\times n$ matrix with rational entries A satisfies*

$$^tA\cdot A=mI+\lambda J$$

where m is a positive integer and λ is a rational number, then the equation

$$x^2=my^2+(-1)^{(n-1)/2}\lambda z^2$$

must have a solution in integers x, y, z, not all zero.

Remark 1. Since $(\det A)^2=\det({}^tA\cdot A)=(m+n\lambda)m^{n-1}$, A is non-singular if and only if $m+n\lambda>0$. Note that this theorem holds even if $m+n\lambda=0$.

Remark 2. If $m+n\lambda>0$, the converse of this theorem is true, that is, a rational matrix A satisfying ${}^tA\cdot A=mI+\lambda J$ does esist whenever the equation has an integral solution. The proof needs the Hasse-Minkowsky theorem (cf. [3]).

PROOF. Putting $\boldsymbol{x}=\begin{bmatrix}x_1\\ \vdots\\ x_n\end{bmatrix}$, ${}^tA\cdot A$ defines the following quadratic form over rationals:

$${}^t\boldsymbol{x}({}^tA\cdot A)\boldsymbol{x}=m(x_1^2+\cdots+x_n^2)+\lambda(x_1+\cdots+x_n)^2.$$

Putting $A\boldsymbol{x}=\boldsymbol{z}=\begin{bmatrix}z_1\\ \vdots\\ z_n\end{bmatrix}$, we have

$$(*)\qquad z_1^2+\cdots+z_n^2=m(x_1^2+\cdots+x_n^2)+\lambda(x_1+\cdots+x_n)^2.$$

According to Lagrange's four square theorem in elementary number theory (cf. [4]), m can be written as the sum of (at most) four squares as $m=m_1^2+m_2^2+m_3^2+m_4^2$. Consider the following matrix:

$$H=\begin{pmatrix} m_1 & m_2 & m_3 & m_4 \\ m_2 & -m_1 & m_4 & -m_3 \\ m_3 & -m_4 & -m_1 & m_2 \\ m_4 & m_3 & -m_2 & -m_1 \end{pmatrix}.$$

We have ${}^tH\cdot H=mI$, so that if $H\begin{bmatrix} x_1 \\ \vdots \\ x_4 \end{bmatrix}=\begin{bmatrix} y_1 \\ \vdots \\ y_4 \end{bmatrix}$ then $y_1^2+\cdots+y_4^2=[x_1\cdots x_4]{}^tH\cdot H\begin{bmatrix} x_1 \\ \vdots \\ x_4 \end{bmatrix}=m(x_1^2+\cdots+x_4^2)$.

Suppose first that $n\equiv 1 \pmod{4}$. Consider the following $n\times n$ non-singular matrix:

$$\boldsymbol{M}=\begin{pmatrix} H & 0 & \cdots & \cdots & 0 \\ 0 & H & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & H & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

and put $\boldsymbol{Mx}=\boldsymbol{y}=\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ and $w=x_1+\cdots+x_n$. From (*), we get

$$(**)\qquad z_1^2+\cdots+z_n^2=y_1^2+\cdots+y_{n-1}^2+my_n^2+\lambda w^2.$$

Using $(n+1)\times n$ matrix $A'=\begin{bmatrix} A \\ 1\cdots 1 \end{bmatrix}$, we have $\begin{bmatrix} z_1 \\ \vdots \\ z_n \\ w \end{bmatrix}=A'M^{-1}\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$, so that $z_1,\cdots z_n$ and w are rational linear combinations of $y_1,\cdots,y_n$. Put $A'M^{-1}=(b_{ij})$ $(1\leqq i\leqq n+1, 1\leqq j\leqq n)$. If $b_{11}\neq 1$, we set

$$y_1=(1-b_{11})^{-1}(b_{12}y_2+\cdots+b_{1n}y_n),$$

while if $b_{11}=1$ we set

$$y_1=-(1+b_{11})^{-1}(b_{12}y_2+\cdots+b_{1n}y_n).$$

In both cases, we have $z_1^2=y_1^2$ and z_2 is a rational linear combination of $y_2,\cdots,y_n$. In the same way as above, we fix y_2 as a rational linear combination of $y_3, \cdots, y_n$, such as $z_2^2 = y_2^2$. Continuing this, we obtain $y_1, \cdots, y_{n-1}$, $z_1, \cdots, z_n$ and w as rational multiples of y_n, satisfying $z_i^2 = y_i^2$ $(1 \leqq i \leqq n-1)$. Choose any non-zero rational value for y_n. In the relation obtained above, all remaining variables $z_1, \cdots, z_n$, $y_1, \cdots, y_{n-1}$ and w take rational values, and substituting these values in (**), we obtain

$$z_n^2 = m y_n^2 + \lambda w^2 .$$

Multiplying by a suitable integer we have an integral solution for the equation, and the theorem is proved in the case $n \equiv 1$ (mod. 4).

In the case $n \equiv 3$ (mod. 4), we add an extra term $m x_{n+1}^2$ to both sides of identity (*) and put

$$M = \begin{bmatrix} H & & \\ & \ddots & \\ & & H \end{bmatrix}, \quad A' = \begin{bmatrix} & A & & 0 \\ & & & \vdots \\ 1 & \cdots & 1 & 0 \end{bmatrix} \quad \text{and} \quad M \begin{bmatrix} x_1 \\ \vdots \\ x_{n+1} \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_{n+1} \end{bmatrix},$$

Then we have $\begin{bmatrix} z_1 \\ \vdots \\ z_n \\ w \end{bmatrix} = A' M^{-1} \begin{bmatrix} y_1 \\ \vdots \\ y_{n+1} \end{bmatrix}$ and $z_1^2 + \cdots + z_n^2 + m x_{n+1}^2 = y_1^2 + \cdots + y_{n+1}^2 + \lambda w^2$.

Repeat the argument given above, we obtain $m x_{n+1}^2 = y_{n+1}^2 + \lambda w^2$. The proof is now completed.

THEOREM 2. *If* $n \equiv 1$ (mod. 4) *and an* $n \times n$ *matrix with rational entries* A *satisfies either* ${}^tA \cdot A = nI + (n-1)J$ *or* ${}^tA \cdot A = nI - J$, *then* n *must be a sum of two squares of integers.*

PROOF. Note that A is singular in the latter case. By Theorem 1 either $x^2 = ny^2 + (n-1)z^2$ or $x^2 = ny^2 - z^2$ has an integral solution. Hence $n(y^2 + z^2) = x^2 + z^2$ or $ny^2 = x^2 + z^2$ holds. From elementary number theory it follows that n is a sum of two squares.

THEOREM 3. *Let* Γ *be a strongly regular graph with parameters* (n, a, c, d), *where* n *is the number of vertices,* a *the valency, and the number of vertices adjacent to* p_1 *and* p_2 *is* c *or* d *according as* p_1 *and* p_2 *are adjacent or non-adjacent.*

If n *is odd, then the equation*

$$x^2 = (4(a-d) + (c-d)^2) y^2 + (-1)^{(n-1)/2} 4 d z^2$$

must have a solution in integers x, y, z, *not all zero.*

PROOF. Let A be the adjacency matrix of Γ. Then A satisfies

$$AJ = JA = aJ ,$$

$$A^2 = (c-d)A + (a-d)I + dJ .$$

Putting $B=2A-(c-d)I$, we have

$$B^2=(4(a-d)+(c-d)^2)I+4dJ.$$

By Theorem 1, the equation stated above has an integral solution.

COROLLARY. *If a strongly regular graph has parameters* $(4d+1, 2d, d-1, d)$, *then* n *must be a sum of two squares.*

PROOF. This follows immediately from Theorem 3 and Theorem 2. Or, if we put $B=2A+I-J$ where A is the adjacency matrix of this graph, then we have $B^2=nI-J$. Again from Theorem 2, the result follows.

References

[1] Biggs, N. L. and White, A. T.: Permutation Groups and Combinatorial Structures. L. M. S. Lecture Note 33, C. U. P., 1979.
[2] Cameron, P. J. and Lint, J. H. van: Graphs, Codes and Designs. L. M. S. Lecture Note 43, C. U. P., 1980.
[3] Hall, M. Jr.: Combinatorial Theory. Wiley-Interscience, New York, 1986.
[4] Hardy, G. H. and Wright, E. M.: An Introduction to the Theory of Numbers. Oxford Univ. Press, 1979.