A Minimal Critical Set of a Class of Youden Squares

Lakoa Fitina, Kenneth G Russell and Jennifer Seberry
Centre for Computer Security Research
School of Mathematics & Applied Statistics
and
School of IT & Computer Science
University of Wollongong
NSW 2522
Australia

Abstract

We consider the Youden square formed by deleting one row of a $v \times v$ back-circulant Latin square and establish a critical set that contains a number of elements which is equal to $v^2/4$ (v even) or $(v^2-1)/4$ (v odd). We show that this critical set is minimal, for v even.

Key words and phrases: access schemes, Latin square, secret sharing
AMS Subject Classification: Primary 62K10, 62K99; Secondary 05B15

1 Introduction

The name *Youden square* is used by statisticians to describe a $k \times v$ array, Y (where $2 \leq k < v$, so the array is actually a rectangle), each of whose cells contains an object from the set $\{1, 2, \ldots, v\}$, such that:

(i) each of the objects $1, 2, \ldots, v$ occurs precisely once in each row of Y and at most once in each column of Y, and

(ii) the arrangement of the objects $1, 2, \ldots, v$ within the columns of Y is that of a balanced incomplete block design, namely, each pair of distinct objects occurs in λ blocks, where λ is an integer.

We use the notation "element $(i, j; x)$" to denote the triple which has x in position (i, j) of the Youden square.

A *critical set* of a Youden square Y is a set $\mathcal{C} = \{(i, j; x)\}$, of cardinality c, where $i \in \{1, 2, \ldots, k\}; j, x \in \{1, 2, \ldots, v\}$, such that:

(i) Y is the only $k \times v$ Youden square which has the element x in cell (i, j) for each $(i, j; x) \in \mathcal{C}$, and

(ii) no proper subset of $\mathcal{C}$ satisfies (i).

A *critical set*, $\mathcal{C}$, is the minimal partial information from which we can reconstruct the whole structure, Y, uniquely. A *minimal critical set (mcs)* of a Youden square Y is a critical set of minimum cardinality whereas a *largest critical set (lcs)* is a critical set of maximum cardinality.

The study of similar sets in *Latin squares* arose from a problem at the Rothamsted Experimental Station [7].

A $v \times v$ back-circulant Latin square is one with initial row $1, 2, 3, \ldots, v$ and with subsequent rows formed by translating the previous row one element to the left. In this note we study the critical sets of the class of Youden squares formed by deleting one row from a back-circulant Latin square. Such Youden squares have parameters $k = v - 1$ and $\lambda = v - 2$. We say that the information content of a Youden square is the information content of the critical set plus the information content of the rules for constructing a Youden square.

This is the first paper to consider critical sets of Youden squares. However, critical sets of Latin squares, and defining sets of graph colourings and Latin rectangles, have been considered by a number of authors; see for instance [2], [3], [6], [7], [10], [11].

Critical sets are of importance in a study of secret sharing schemes. Secret sharing depends on distributing a secret among a group of participants, individuals or entities, so that only pre-designated collections of participants are able to recreate the secret by collectively combining their *shares* of the secret. See for instance [5], [8], [9].

Structures which have rules for completion such as balanced incomplete block designs, Latin squares, F-squares, Youden squares, regular graph colourings, finite geometries, block designs and difference sets may all be used to construct hierarchical and compartmentalized secret sharing schemes. This is discussed more fully in [1], [4], [8] for example.

2 Critical sets

Let $m = [v/2]$, where $[x]$ represents the greatest integer not exceeding x. Form the $(v-1) \times v$ Youden square, Y_v, by deleting the $(m+1)$st row of the $v \times v$ back-circulant Latin square. Then, within Y_v, delete all but the first $(m+1-i)$ objects in row i $(i = 1, \ldots, m)$ and delete all but the last j elements in row $m+j$ $(j = 1, \ldots, v-1-m)$. Call this resulting array Y_v^*. Each row of Y_v^* contains at least one element, and exactly one column of Y_v^* is completely empty. The non-empty cells of Y_v^* form one triangle containing $m(m+1)/2$ elements in the top left-hand corner, and a second triangle containing $(v-1-m)(v-m)/2$ elements in the bottom right-hand corner. It is simple to show that Y_v^* has $v^2/4$ non-empty cells if v is even, and $(v^2-1)/4$ non-empty cells if v is odd. Denote by $\mathcal{C}_v$ the set of non-empty cells of Y_v^*. We claim that $\mathcal{C}_v$ forms a critical set for Y_v.

We call $\mathcal{C}_v$, with two triangle shapes of elements, the *standard form of the critical set* of Y_v. We refer to the two triangles as the *upper left* and *lower right* triangles.

Example and Notation. We show below Y_6^* and Y_7^*. Two additional cells are displayed on the extreme right of the layouts. The size of the critical set is written in the upper cell and the number of elements in the completed square in the lower cell.

1	2	3				9
2	3					
3						
					4	
				4	5	30

1	2	3					12
2	3						
3							
						4	
					4	5	
				4	5	6	42

It is well known from [2] that:

Theorem 1 *The array which consists of C_v augmented by a row of zeros is a critical set for the $v \times v$ back-circulant Latin square.*

Theorem 2 *A Youden square Y of order $(v-1) \times v$ can be uniquely extended to a Latin square L of order v. L is called the* extension *of Y.*

Proof. Each column of Y lacks precisely one element from the set $\{1, 2, \ldots, v\}$. Form the v^{th} row by placing, in cell (v, j), the element missing from column j. This row is uniquely obtained. □

Corollary 1 *A critical set $\mathcal{C}$ for a Youden square Y of order $(v-1) \times v$ must also, after augmentation by a v^{th} row of empty cells, be a critical set for the Latin square extension, L, of Y.*

Proof. Since $\mathcal{C}$ is uniquely completable to Y, its augmentation must also, by Theorem 2, be uniquely completable to L. Suppose an element, x, is deleted from $\mathcal{C}$. Then $\mathcal{C} \setminus \{x\}$ must complete to at least two Youden squares and, by Theorem 2, each Youden square has a unique extension. Thus the augmentation of $\mathcal{C}$ is also a critical set for L. □

Theorem 3 *Let L be a Latin square of order v. Let $\mathcal{K}$ be a critical set of L, which has no elements in row r, say, and let $\mathcal{K}_r^*$ be the array formed by deleting row r of $\mathcal{K}$. Then the Youden square Y, formed by the removal from L of row r, has $\mathcal{K}_r^*$ as a critical set.*
Further, if $\mathcal{K}$ is minimal for L,, then $\mathcal{K}_r^*$ is minimal for Y.

Proof. Since $\mathcal{K}_r^* \subseteq Y$, therefore $\mathcal{K}_r^*$ must complete uniquely to Y. If an element $x = (i, j; k)$ of $\mathcal{K}_r^*$ is deleted, then $\mathcal{K}_r^* \setminus \{x\}$ extends to at least two Latin squares. These Latin squares must differ in the entry corresponding to cell (i, j) of $\mathcal{K}_r^*$. Since this cell does not occur in row r, the removal of this element and of row r results in two distinct Youden squares. That is, $\mathcal{K}_r^*$ must be a critical set of Y.
Suppose $\mathcal{K}_r^*$ is not minimal for Y. Then there exists a critical set $\mathcal{M}_r^*$ of Y, such that $|\mathcal{M}_r^*| < |\mathcal{K}_r^*|$. By Corollary 1, the extension $\mathcal{M}$ of $\mathcal{M}_r^*$ is also a critical set of L. But then $\mathcal{K}$ is not minimal for L, a contradiction. □

Corollary 2 *If v is even, then $\mathcal{C}_v$ is a minimal critical set for Y.*

Proof. It is shown in [2], for example, that, if v is even, then the array formed by augmenting $\mathcal{C}_v$ by a row of zeros is a minimal critical set for the back-circulant $v \times v$ Latin square. Thus, by the theorem above, $\mathcal{C}_v$ is a minimal critical set for Y. □

We conjecture that $\mathcal{C}_v$ forms a minimal critical set for Y_v, for v odd. The basis for this conjecture includes the following: a Youden square cannot be formed uniquely from a partial Youden square which leaves two columns (or rows) blank, since we cannot know which column should contain a particular set of k objects (nor which row should contain a particular permutation of v objects). Consequently, Y_3 could not have a critical set of only one element, so $\mathcal{C}_3$ forms a minimal critical set for Y_3.

A computer program was used to generate all $\binom{20}{5}$ possible critical sets of five elements for Y_5 to see whether any such set could be uniquely completed to form the appropriate Youden square. None of the possible critical sets could be uniquely completed.

Remark. The preceding discussion considered a Youden square Y_v formed by deletion of the $(m+1)$st row of the $v \times v$ back-circulant Latin square. However, the decision to delete the $(m+1)$st row was made only to simplify our proof. It is easy to verify that a Youden square formed by deleting some row of the Latin square other than the $(m+1)$st can be obtained from Y_v merely by reordering the rows of Y_v and then by cycling the order of the columns of Y_v. Consequently, a critical set of $v^2/4$ elements (for v even) or $(v^2-1)/4$ elements (for v odd) for this new Youden square can be obtained by applying the same reordering of rows and columns to Y_v^*.

Thus, although the preceding results were obtained specifically for the Youden square obtained by deleting the $(m+1)$st row of the $v \times v$ back-circulant Latin square, they apply to a Youden square formed by deleting any one row of that Latin square.

References

[1] G. Chaudhry, H. Ghodosi and J. Seberry, Perfect secret sharing schemes from Room squares. *J Combin. Math. Combin. Comput.* **28** (1998), 55–61.

[2] J. Cooper, D. Donovan and J. Seberry, Latin squares and critical sets of minimal size. *Australas. J Combin.* **4** (1991), 113–120.

[3] D. Curran and G.H.J. van Rees, *Critical sets in Latin squares.* Proc. Eighth Manitoba Conference on Numerical Math. and Computing, (1978), 165–168.

[4] Greg Gamble, Barbara M Maenhaut, Jennifer Seberry and Anne Penfold Street, Further results on strongbox secured secret sharing schemes, *Utilitas Math.* **66** (2004), 187–215.

[5] Hossein Ghodosi, Josef Pieprzyk and Rei Safavi-Naini, *Secret Sharing in multi level and compartmented groups*, in “Information and Privacy”, eds C Boyd and E Dawson, *LNCS*, Springer-Verlag, Berlin, Vol 1438, (1998), 367–378.

[6] E.S. Mahmoodian, R. Naserasr and M. Zaker, Defining sets in vertex colourings of graphs and latin rectangles, *Discrete Math.* **167/168** (1997), 451–460.

[7] J. Nelder. Critical sets in Latin squares, CSIRO Div. of Math. and Stats. *Newsletter* **38** (1977).

[8] Jennifer Seberry and Anne Penfold Street, Strongbox secured secret sharing schemes, *Utilitas Math.* **57** (2000), 147–163.

[9] Simmons, G J (Ed.), 1991. Contemporary Cryptology: The Science of Information Integrity. IEEE Press, Piscataway, NJ.

[10] B. Smetaniuk, On the minimal critical set of a Latin square, *Utilitas Math.* **16** (1979), 97–100.

[11] D.R. Stinson and G.H.J. van Rees, Some large critical sets, *Congr. Numer.* **34** (1982), 441–456.