INFLUENCE OF ENTRIES IN CRITICAL SETS OF ROOM SQUARES

Ghulam Chaudhry and Jennifer Seberry

School of IT and Computer Science, The University of Wollongong, Wollongong, NSW 2522, AUSTRALIA

We establish the notions of influence, power and strong box in the critical sets of Room squares and study their properties.

Indexing terms: Room square, critical set, influence, power, strong box, secret sharing.

1 Introduction

We consider structures which have rules for completion such as balanced incomplete block designs, Latin squares, Rooms squares, F-squares, Youden squares, regular graphs, colourings, finite geometries and difference sets. In particular we are concerned with the problem of unique completion of structures given partial information. If the partial structure can be uniquely completed then this partial structure together with the rules contains the same information as the final structure. In this paper, we study the information inherent in partial Room squares, where it is not possible to uniquely complete the square. We study the influence and power of parts of the partial square on the unique completion of larger partial squares containing those parts. That part of Room square, called the strong box, which is inaccessible to all the q-subsets of a critical set may be thought to contain the secret information. We study the size of the secret which will be used to model secret sharing schemes.

A Room square R of order r is an r $\times$ *r* array each of whose cells may either be empty or contain an unordered pair of objects 0, 1, 2, …, r subject to the following conditions:

(i) each of the objects 0, 1, 2, …, r occurs precisely once in each row of R and precisely once in each column of R, and

(ii) every possible unordered pair of objects occurs precisely once in the whole array.

Theorem 1 (Mullin and Wallis [6]) There exists a Room square of every odd order greater than or equal to 7.

A partial Room square P of order r is an r × *r* array each of whose cells may either be empty or contain an unordered pair of objects 0, 1, 2, …, r, subject to the following conditions:

(i) each of the objects 0, 1, 2, …, r occurs at most once in each row of R and at most once in each column of R, and

(ii) every possible unordered pair of objects occurs at most once in the whole array.

A critical set $Q = [Q_1, Q_2, Q_3, \ldots, Q_c]$, $|Q| = c$, in a Room square R of order r, is a set of quadruples $Q_a = [i, j; x, y]$ such that

(i) R is the only Room square of order r which has the entry (x, y) at the position (i, j), for each Q_a.

(ii) No proper subset of Q satisfies 1.

In Q_a, (i, j) shows the position of (x, y) in R where (x, y) may either be a pair of distinct integers or an empty position expressed as (–). That is, Q provides minimal information from which R can be reconstructed uniquely. A minimal critical set of a Room square R of order r is a critical set of minimum cardinality. A maximal critical set is a critical set of maximum cardinality.

Example 1: A critical set of a Room square $R7_5$ of order 7 given by Wallis in [9] and its completion.

0 1	* *	* *	* *	* *	* *	* *
* *	* *	* *	* *	* *	3 7	* *
2 7	5 6	* *	* *	* *	* *	* *
* *	* *	* *	* *	* *	* *	2 6
* *	4 7	* *	* *	0 5	* *	* *
* *	* *	* *	1 7	* *	* *	* *
* *	* *	* *	– –	2 3	4 5	* *

0 1	– –	– –	2 5	6 7	– –	3 4
4 6	0 2	– –	– –	– –	3 7	1 5
2 7	5 6	0 3	– –	1 4	– –	– –
– –	1 3	5 7	0 4	– –	– –	2 6
– –	4 7	– –	3 6	0 5	1 2	– –
3 5	– –	2 4	1 7	– –	0 6	– –
– –	– –	1 6	– –	2 3	4 5	0 7

where "**" show the unknown entries and "–"show empty cells in the Room square.

2 Power and Influence

We study the information inherent in partial Room squares and their critical sets where it is not possible to uniquely complete the Room square. In a critical set Q of size q, of a Room square R of order r, every entry has a different importance in the reconstruction of R. If we delete an entry from Q and try to reconstruct R, then the remaining (q – 1) entries will be able to recover some of the entries of R. The power of an entry, P, is the number of ways in which the Room square can be completed with that entry removed from Q. The power of a a set, $\mathcal{P}$, is the number of ways in which the Room square can be completed with that set of entries removed from Q.

The influence of an entry, I, is the number of entries in the Room square which cannot be filled with that entry removed from Q. The influence of a set, $\tilde{I}$, is the number of entries in the Room square which cannot be filled with that set of entries removed from Q. The deleted entry or set of entries from Q which allows minimum number of fillings in R is called the most influential and is denoted by I_m. The deleted entry or set of entries from Q which allows maximum number of fillings in R is called the least influential and is denoted by I_l. A deleted entry or set of entries without which we cannot recover any entry in R has perfect influence. We denote it by I_p.

The purpose of studying power and influence is to find the part of the Room square, the strong box, which cannot be uniquely completed by any set of q-subsets of the critical set of a Room square. The intersection of the cells of the influences of all the entries, one at a time, in the critical set is called the strong box. So no coalition of fewer than all the q-subsets of a critical set Q of size q can recover any entry from the strong box of Room square. We illustrate above definitions with examples given below:

Example2: In the example1 above, the size of the critical set is 11. In the following table, we compute the influence of all eleven entries by deleting each entry, one at a time:

Deleted entry	Fillings	Influence	Remarks
1,1;0,1	10	38	I_m & I_p
2,6;3,7	16	32	
3,1;2,7	14	34	
3,2;5,6	13	35	
4,7;2,6	14	34	
5,2;4,7	14	34	
5,5;0,5	18	30	I_l
6,4;1,7	16	32	
7,4;– –	16	32	
7,5;2,3	13	35	
7,6;4,5	12	36	

In this table, the entry (1,1;0,1) has the most influence, it is also perfect as the remaining ten entries in Q do not permit the reconstruction of even a single entry of R. The entry (5,5;0,5) has the least influence because it reveals the most information about R. These most and least influence sets are shown in the squares given below respectively:

	* *	* *	* *	* *	* *	* *
* *	* *	* *	* *	* *		* *
		* *	* *	* *	* *	* *
* *	* *	* *	* *	* *	* *	
* *		* *	* *		* *	* *
* *	* *	* *		* *	* *	* *
* *	* *	* *				* *

		* *	* *	* *		* *
* *	* *	* *	* *	* *		* *
		* *	* *	* *		* *
* *	* *	* *	* *	* *		
* *		* *	* *		* *	* *
* *	* *	* *		* *	* *	* *

The strong box of the Room square in example 1 consists of 29 unknown cells with "* *" as given below. These cells cannot be computed by any subset of the critical set:

		* *	* *	* *		* *
* *	* *	* *	* *	* *		* *
		* *	* *	* *		* *
* *	* *	* *	* *	* *		
* *			* *		* *	* *
* *	* *	* *		* *	* *	* *

After the permutation of rows and columns, the strong box has been shifted to the upper left corner of the square as shown below:

* *	* *	* *	* *	* *	* *	
* *	* *	* *	* *	* *	* *	
* *	* *	* *		* *	* *	* *
* *	* *	* *	* *			
* *	* *		* *			
		* *	* *	* *		* *

Example 3: We take a critical set of size 10 of another Room square $R7_1$ of order 7 given by Wallis in [9] and compute the influence of all ten entries by deleting one entry at a time. In this example, we could not find an instance of perfect influence by the deletion of just one entry, so we computed perfect influences by deleting two entries at a time. The influences are given in the table below:

Deleted entry/set	Fillings	Influence	Remarks
1,4;2,5	24	24	I_l
1,5;4,6	11	37	I_m
2,3;1,5	12	36	
3,3;0,3	15	33	
4,5;2,7	16	32	
5,2;1,4	19	29	
5,7;2,3	19	29	
7,1;3,4	19	29	
7,6;1,2	18	30	
7,7;0,7	13	35	

1,5;4,6 7,7;0,7	8	39	I_p
2,3;1,5 7,7;0,7	8	39	I_p

In this example, most of the entries have differing influence. No single entry has a perfect influence. A set of two entries need both to be deleted to get perfect influence as shown in the table above. The strong box of the Room square, having this critical set, consists of 20 unknown cells.

Similarly we have computed the influences for other Room squares of order 7 and some examples of Room squares of order 9. In most examples of order 7, we need to delete two entries from the critical set to get perfect influence, but there might be other critical sets where one entry is sufficient to obtain perfect influence. We had to delete a set of three entries from a critical set of a Room square of order 9 to attain perfect influence. We have found that each entry in critical set has different influence/importance, that is, some entries are more influential than others and vice-versa.

We have noticed that deletion of one entry from a critical set of a Room square of order 7 gives us perfect influence whereas in backcirculant Latin squares, F-squares and Youden squares, we have to delete two or more entries to get perfect influence. We have also noticed that sizes of the strong boxes in Room squares are much larger than those of Latin squares, F-squares and Youden squares. The size of the strong box varies from critical set to critical set in Room squares, but roughly it is of size $\frac{n^2}{2}$. This makes Room squares more useful in applications as so little extra information can be gleaned. We have also observed that empty cells have less influence than pairs of integers in Room squares in the examples we studied.

3 Secret Sharing

A secret sharing scheme based on critical sets would have q sets of quadruples associated with the critical set distributed as shares. We allow the secret to be some function of the cells of quadruples in the strong box. If the secret is the same size as each share we obtain an ideal secret sharing scheme. By definition we have that no q – 1 shares can recover the secret, that is, an outsider has the same probability of guessing the secret as an insider.

We now need to consider the possibility of guessing the contents of the strong box. The worst case is when q – 1 cheaters have colluded to get as much information as they can before guessing the contents of the strong box. The power of the strong box, that is, the number of possible completions of the strong box to Room squares, is a NPC problem as proved

by Colbourn, Colbourn and Stinson [5], that is “finding a completion of P is equivalent to finding a decomposition of G(P) into edge-disjoint triangles of the defect graph”. Using this observation, it has been shown that, in general, completing partial latin squares is NP-complete. Furthermore, given a partial latin square and one completion, deciding whether a second completion exists is also NP-complete. The same applies to Room squares as these are constructed from the pairs of mutually orthogonal latin squares.

We note that most of the entries in the critical sets have differing influence, so an hierarchical scheme can be built as per the importance of the shares held by the shareholders. In example 2, the shareholder having the share containing quadruple with (1, 1;0, 1) has perfect influence and can single-handedly prevent reconstruction of any entry in the Room square whereas the share with (5, 5;0, 5) reveals eight entries of the Room square.

4 Conclusion

The results in this paper have been produced computationally. One of the open problems is to generalise these results and construct hierarchical structures of influences in Room squares and compute the power of the strong box if possible. These type of combinatorial structures can be used in secret sharing schemes, particularly hierarchical schemes where some participants are more important than others. The size of the strong box in Room squares is much larger than those of Latin squares, F-squares and Youden squares, so we can conjecture that Room squares are more useful for applications where little information can be gleaned.

References

[1] G. R. Chaudhry and J. Seberry. Minimal critical set of a Room square of order 7. Bulletin of the ICA, 20 (1997), pp.90.

[2] G. R. Chaudhry and J. Seberry. Room squares: critical sets and their bounds. 3rd International Conference on Combina. Math. and Combin. Comput. (3ICCMCC'97), Melbourne, Australia, July 1997.

[3] G. R. Chaudhry and J. Seberry. Secret sharing schemes based on Room squares. Combinatorics, Complexity and Logic, Proceedings of DMTCS'96, Springer-Verlag Singapore (1996), pp. 158 -167.

[4] G. R. Chaudhry, H. Ghodosi and J. Seberry. Perfect secret sharing schemes from Room squares, J. Combin. Math. and Combin. Computing (JCMCC), Canada 28 (1998), pp.55-61.

[5] C.J. Colbourn, M.J. Colbourn and D. R. Stinson. The computational complexity of recognising critical sets, in proc. First Southeast Asian Graph Theory Colloquium, Lecture Notes in Mathematics 1073 (1984), 248-253;(Springer-Verlag, Berlin, Heidelberg, NewYork).

[6] R.C. Mullin and W.D. Wallis. The existence of Room squares. Aequa. Math. 13 (1975), 1-7.

[7] J .Seberry and A.P. Street. A secret sharing strong box scheme (in preparation).

[8] J. Seberry and A.P. Street. A secret sharing scheme based on computational infeasibility (submitted).

[9] W.D. Wallis, A.P. Street and J.S. Wallis. Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices. Lect.Notes Math.293 (1972).