Math/CS 103	Professor: Padraic Bartlett

Minilecture 11: Secret-Sharing Schemes

Week 8	*UCSB 2014*

Latin squares can also be used for **secret-sharing schemes**, which we define here:

Definition. A (t, k)-**secret-sharing scheme** is a system where k pieces of information about some secret key K are distributed to various people, so that

- the key K can be reconstructed from the knowledge of any t pieces of information, and
- the key K cannot be reconstructed from the knowledge of less than t pieces of information (no matter what those pieces are!)

We can make these via Latin squares as follows:

Definition. A **critical set** in a $n \times n$ Latin square L is a collection of triples

$$C = \{[(i, j), k] \mid i, j, k \in \{1, \dots n\}\},$$

such that the following properties hold:

1. L is the only Latin square of order n that has symbol k in cell (i, j), for each triple $[(i, j), k]$.
2. If we take any proper subset of C, property (a) does not hold for that subset.

For example, consider the Latin square

$$L = \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 2 & 3 & 1 \\ \hline 3 & 1 & 2 \\ \hline \end{array}.$$

One critical set for L is the following:

$$L = \begin{array}{|c|c|c|} \hline & & \\ \hline 2 & & \\ \hline & 1 & \\ \hline \end{array}.$$

We say that a critical set C is **minimal** for L if there is no other critical set of smaller size for L.

We can use these minimal critical sets to construct secret-sharing systems! To see how, consider the following example. Let L be the 3×3 Latin square we created earlier. It is clear that the critical set we constructed is minimal, because specifying just one cell of a 3×3 Latin square does not uniquely specify it. Furthermore, if we pick any two cells in L that don't share the same row/column/symbol, it's hopefully relatively clear that they specify a critical set (prove this if you don't see why.)

Given these observations, consider the set

$$S = \{[(2, 1), 2], [(3, 2), 1], [(1, 3), 3]\}.$$

Any subset of two elements of S forms a critical set for L! Therefore, if we consider L to be the key K and the elements of S to be the pieces k_1, k_2, k_3 of that key, we have constructed a $(2, 3)$ secret-sharing system!

Generalizing this is part of this class's HW!