Lec23 Latin squares

A Latin square of order n is a $n \times n$ array, each cell containing one entry from the set $[n]$, with the property that each element of $[n]$ occurs once in each row and once in each column of the array.

Notice that each row and each column is a permutation of $[n]$. We may think a $n \times n$ latin square as a 1-factorization of $K_{n,n}$.

Prop: The number of Latin squares of order n is at least $n!(n-1)! \cdot 2! \cdot 1!$. (proof: use Hall's theorem from one row to n rows)

Trivially, there are at most n^{n^2} Latin squares of order n, since each cell has at most n choices. Note that each row has at most $n!$ choices, there are at most $(n!)^n$ Latin squares of order n. One can even do better by noting that the other rows are derangements of first row, so there are at most $n! \cdot (d(n))^{n-1}$ Latin squares of order n, where $d(n)$ is the number of derangements of $[n]$ (which is approximately $n!/e$).

Two Latin squares of order n have in total n^2 pairs of positions. They are orthogonal if the pairs are all different. Thus, any pair (i, j) with $i, j \in [n]$ appear once and exactly once in the two Latin squares.

Def: A family of Latin squares of order n are mutually orthogonal (MOLS) if any pair of them are pairwise orthogonal.

Prop: there are at most $n-1$ MOLS of order n. (Proof: Let's normalize the LS so that the first rows are $1234 \cdots n$. Then in a particular position below the first row, the values in all Latin squares in the family must be distinct. They also must be different from the column index. There are only $n-1$ such values and thus at most $n-1$ squares in the family.)

A MOLS of order n is a complete family if the size of the family is $n-1$. In this case, it is called $MOLS(n, n-1)$.

When does a MOLS(n, n-1) exist?

Theorem (Moore 1896, Bose 1938, Stevens 1939) If n is a power of a prime, then there is a complete family $MOLS(n, n-1)$.

Proof: For any power of prime $n = p^m$, there is a finite field F_n. Let $x_1, x_2, \ldots, x_n$ be the elements of F_n with x_n be the additive identity (or 0). For each $k \in [n-1]$, we put $x_k x_i + x_j$ in the (i, j) position. So thus defines $n-1$ squares. Now we can show there are all Latin squares and also pairwise orthogonal.

If the pair at (i, j) position in k, l-th Latin square has the same value as pair in (s, t) position in k, l-th Latin squares, then $x_k x_i + x_j = x_k x_s + x_t$ and $x_l x_i + x_j = x_l x_s + x_t$. We get $x_i = x_s$ and $x_j = x_t$.

Theorem (Moore 1896) Given $MOLS(n, h)$ and $MOLS(m, h)$, we can get $MOLS(mn, h)$. (Proof: we crone each cell in one family to a Latin square (a_{ij}, B_t).)

As a corollary, $n = \prod_i p_i^{e_i}$ can be written as a product of prime powers, so we can get a set $\min_i \{p_i^{e_i}\}$ of orthogonal Latin squares of order n.

But when $n = 2(2k+1)$, this method doesn't give any pair of orthogonal Latin squares. Euler conjectured that for any number $n \equiv 2 \mod 4$, there is no orthogonal Latin squares of order n. Let $N(n)$ be the number of orthogonal Latin squares of n. Then $N(2) = 1$, and $N(6) = 1$ (hard), so Euler was right on those two. But $N(n) > 1$ for any $n > 6$. But it not know if $N(10) \geq 3$.