Combinatorics and Graph Theory I

Exercise sheet 9: Latin squares, Ramsey theory

3 May 2017

1.

(i) Prove that the $n \times n$ array L whose (i, j)-entry is defined by

$$L(i, j) = i + j \pmod n$$

is a Latin square.

$L(i, j) = L(i', j)$ iff $i + j = i' + j$ iff $i = i'$, so columns contain distinct elements. Similarly, $L(i, j) = L(i, j')$ iff $i + j = i + j'$ iff $j = j'$, so rows contain distinct elements.

(ii) Let p be a prime and $1 \leq k \leq p - 1$. Prove that the $p \times p$ array L_k whose (i, j)-entry is defined by

$$L_k(i, j) = ki + j \pmod p$$

defines a Latin square.

$L_k(i, j) = L_k(i', j)$ iff $ki + j = ki' + j$ iff $ki = ki'$ iff $i = i'$ (the last since k is non-zero mod p and hence invertible), so columns contain distinct elements. Similarly, $L_k(i, j) = L_k(i, j')$ iff $ki + j = ki + j'$ iff $j = j'$, so rows contain distinct elements.

(iii) Prove that when $k \neq \ell$ the Latin squares L_k and L_ℓ defined in (ii) are orthogonal.

If the Latin squares L_k and L_ℓ have the same pair of symbols (a, b) in positions (i, j) and (i', j') then

$$ki + j = a, \quad \ell i + j = b,$$

$$ki' + j' = a, \quad \ell i' + j' = b.$$

It follows that

$$k(i - i') = j' - j, \quad \ell(i - i') = j' - j$$

. If $i - i' = 0$ then $j' - j = 0$ and the two positions are the same. If not, then $i - i'$ is invertible and

$$k = (i - i')^{-1}(j' - j) = \ell,$$

so that $k = \ell$. Hence if $k \neq \ell$ then L_k and L_ℓ are orthogonal.

[In the answers to (ii) and (iii) all the equalities stand for equivalence modulo p (or equality of elements in $\mathbb{Z}_p$).] [Adaptation of Matoušek & Nešetřil, *Invitation to Discrete Mathematics*, 2nd ed. 9.3, exercise 5, which uses the same construction for a finite field on a prime power number of elements more generally; here the finite field is $\mathbb{Z}_p$.]

2. Use the Pigeonhole Principle to show that any finite graph has at least two vertices of the same degree.

The "boxes" are possible vertex degrees $0, 1, 2, \ldots, n-1$, where n is the number of vertices in the graph, and n vertices are placed into these boxes.

If there is a vertex of degree $n-1$ (box $n-1$ is not empty) then it is joined to all other vertices, so there cannot be a vertex of degree 0. Otherwise there is no vertex of degree $n-1$.

In any event, there are only $n-1$ possible degrees a vertex may have. Since there are n vertices, the Pigeonhole Principle guarantees that some degree d is common to some pair of vertices.

[P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms,* Cambridge Univ. Press, 1994. Chapter 10, exercise 2]

3.

(i) Show that if $n \geq (r-1)(s-1)(t-1)+1$ then any sequence of n real numbers must contain either a strictly increasing subsequence of length r, a strictly decreasing subsequence of length s, or a constant subsequence of length t.

[*First consider the case where only* $(r-1)(s-1)$ *or fewer distinct values occur and apply the Pigeonhole Principle to deduce the existence of a suitably long constant subsequence. Otherwise there are at least* $(r-1)(s-1)+1$ *distinct elements: apply the Erdős–Szekeres theorem as formulated in class.*]

Given $n \geq (r-1)(s-1)+1$ distinct real numbers $x_1, x_2, ..., x_n$, there is either a strictly increasing subsequence of length r, or a strictly decreasing subsequence of length s.

Note that since the terms of the sequence are distinct, an increasing subsequence is strictly increasing, and a decreasing subsequence strictly decreasing.

Proof sketch: For a contradiction, suppose that all increasing subsequences have at most $r-1$ terms, and all decreasing subsequences have at most $s-1$ terms. Define a_i as the longest increasing subsequence ending x_i, and b_i as longest decreasing subsequence ending x_i. By assumption $1 \leq a_i \leq r-1$ and $1 \leq b_i \leq s-1$. Given $i < j$, either $x_i < x_j$, in which case $a_i < a_j$, or $x_i > x_j$, in which case $b_i < b_j$. It follows that the pairs (a_i, b_i) and (a_j, b_j) are different for each $i < j$. In other words the n pairs (a_i, b_i) are distinct, taking values among $(r-1)(s-1)$ possible pairs $\{(a, b) : 1 \leq a \leq r-1, 1 \leq b \leq s-1\}$. But by assumption $n \geq (r-1)(s-1)+1$, and by the Pigeonhole Principle there must be some $i < j$ with $(a_i, b_i) = (a_j, b_j)$. This is the desired contradiction.

An extremal sequence is given by

$$s-1, s-2, \ldots, 2, 1; \quad 2(s-1), 2(s-1)-1, \ldots, s+1., s; \quad \ldots\ldots;$$

$$(r-1)(s-1), (r-1)(s-1)-1, \ldots, (r-2)(s-1)+2, (r-2)(s-1)+1.$$

(This is the concatenation of $(r-1)$ strictly decreasing sequences of length $s-1$, such that later sequences have all their terms greater than those in earlier ones. Any increasing subsequence can have at most one term in each of these sequences, and hence has length at most $r-1$; any decreasing subsequence cannot have terms from two or more of the $r-1$ strictly decreasing subsequences, and so has at most $s-1$ terms.)

A similar, reverse construction is to concatenate increasing sequences of length $r-1$:

$$(r-1)(s-2)+1, (r-1)(s-2)+2, \ldots (r-1)(s-1)-1, (r-1)(s-1); \quad \ldots\ldots;$$

$$r, r+1, \ldots, 2(r-1)-1, 2(r-1); \quad 1, 2, \ldots, r-2, r-1$$

Suppose then $n \geq (r-1)(s-1)(t-1)+1$.

If there are at most $(r-1)(s-1)$ distinct values taken by terms of the sequence then by PHP there is some value taken at least $\lceil\frac{(r-1)(s-1)(t-1)+1}{(r-1)(s-1)}\rceil = t$ times: this defines a constant subsequence of at least t terms.

Otherwise there are at least $(r-1)(s-1)+1$ distinct terms: choose a subsequence of length $(r-1)(s-1)+1$ consisting of distinct terms. By the Erdős–Szekeres theorem there is a strictly increasing subsequence of length r or a strictly decreasing subsequence of length s.

(ii) Show also that the result of (i) is best possible, i.e., construct a sequence of $(r-1)(s-1)(t-1)$ real numbers with no strictly increasing subsequence of length r, no strictly decreasing subsequence of length s, and no constant subsequence of length t.

Take one of the extremal sequences above with each term repeated successively $t-1$ times.

[P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms,* Cambridge Univ. Press, 1994. Chapter 10, exercise 4]