13. COMBINATORIAL DESIGNS

13.1. ARRANGEMENTS

13.1.1. Construction of two orthogonal Latin squares of order 15. First generate two orthogonal Latin squares \((A_1, A_2)\) of order 3 and two orthogonal Latin squares \((B_1, B_2)\) of order 5, such as below. These can be generated from the finite fields \(F_3\) and \(F_5\) by Theorem 13.1.5, since 3 and 5 are prime powers. Here \(F_3 = \{1, 2, 0\}\) and \(F_5 = \{1, 2, 3, 4, 0\}\), leaving the additive identity last as in Theorem 13.1.5.

Next, combine \(A_1\) with \(B_1\) to form \(C_1\), and combine \(A_2\) with \(B_2\) to form \(C_2\), via the construction in the proof of the Moore–MacNeish Theorem (Theorem 13.1.6). That is, in the \((i, j)\)th square block of order 5 in \(C_k\), where \(i, j \in [3]\), place entries with two coordinates, where the first coordinate entry \(i, j\) of \(A_k\) and the second coordinates form a copy of \(B_k\). The resulting squares \(C_1\) and \(C_2\) of order 15 are orthogonal, by the Moore–MacNeish Theorem.

\[
A_1 = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}
\]

\[
B_1 = \begin{pmatrix} 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 3 & 4 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}
\]

13.1.2. A \((v, k, \lambda)\)-design with \(b\) blocks and \(r\) appearances of each vertex exists if and only if a \((v, v - k, b + \lambda - 2r)\)-design exists. Since

\[
(v, v - (v - k), b + (b + \lambda - 2r) - 2(b - r)) = (v, k, \lambda),
\]

it suffices to prove one direction. Let \(B\) be a family of \(k\)-subsets of \([v]\) forming a \((v, k, \lambda)\)-design. Let \(B' = \{X : X \in B\}\). Now \(B'\) is a family of \((v - k)\)-subsets of \([v]\). Each element appears precisely in the sets whose complements it didn’t appear in, so each element appears \(b - r\) times.

Now consider the common appearances. Two elements appear together in the blocks where they both were absent before. Let \(I\) and \(J\) be the indices of the blocks in \(B\) containing elements \(i\) and \(j\), respectively. We have \(T \cap J = T \cup J\), and \(|T \cup J| = |I| + |J| - |I \cap J|\). Since \(|I \cap J| = \lambda\), this yields \(|T \cap J| = b - (2r - \lambda)\). Hence each pair of elements appears in \(b + \lambda - 2r\) common blocks in \(B'\).

13.1.3. If a \((4m - 1, 2m - 1, m - 1)\)-design exists, then there is a Hadamard matrix of order \(4m\). The incidence matrix of the design has order \(4m - 1\), with \(2m - 1\) copies of \(1\) in each column. Any two rows have a \(1\) in \(m - 1\) common columns. Since \((2m - 1)(2m - 2) = (m - 1)(4m - 2)\), the design is symmetric, so also every row has \(2m - 1\) copies of \(1\) and any two columns have a \(1\) in \(m - 1\) common rows.

Convert each \(0\) to a \(-1\), and add an all-1 row at the top and an all-1 column at the left. We claim that the result is a normalized Hadamard matrix. Each row and column has \(2m\) copies of \(1\) and \(2m\) copies of \(-1\). Since two rows of the original matrix have a \(1\) in \(m - 1\) common columns (plus now the new first column), the remaining \(m\) copies of \(1\) in each of the two rows are opposite copies of \(-1\) in their column in the other row, and the final \(m\) columns have \(-1\) in each of the two rows. Hence any two rows have dot product \(0\), which completes the proof.

13.1.4. Use of Paley’s Theorem to construct Hadamard matrices up to order 128. When Hadamard matrices exist of orders \(m\) and \(n\), Proposition 13.1.26 produces a Hadamard matrix of order \(mn\). Paley’s Theorem guarantees a Hadamard matrix of order \(n\) when \(n\) is a multiple of 4 having the form \(2^k(q + 1)\) for some odd prime power \(q\) and nonnegative integer \(k\).

We begin with powers of \(2\), including 4, 8, 16, 32, 64, 128. Similarly, odd prime powers yield 12, 24, 48, 96 (from 5 or 11), 20, 40, 80 (from 9 or 19), 28, 56, 112 (from 13 or 27), 36, 72 (from 17), 52, 104 (from 25), 60, 120 (from 29), 76 (from 37), 84 (from 41), 44, 88 (from 43), 100 (from 49), 108 (from 53), 124 (from 61) and 68 (from 67). Only 92 and 116 are omitted.

13.1.5. Generalized block designs.

\(a\) If each block has size \(k\) and each pair among the \(v\) elements appears together \(\lambda\) times, but the \(i\)th element appears \(r_i\) times, then \(r_1 = \cdots = r_v\).

The \(i\)th element appears \(\lambda\) times with each of the other elements, so it appears in \(\lambda(v - 1)\) pairs. On the other hand, in each of its \(r_i\) appearances it forms pairs with the \(k - 1\) other elements of that block, so it appears in \(r_i(k - 1)\) pairs. Hence \(r_i = \lambda(v - 1)/(k - 1)\), and \(r_i\) is independent of \(i\).

\(b\) Designs with blocks of unequal size. Since the blocks must partition the pairs of elements, they can be viewed as complete subgraphs (not all the same size) decomposing a complete graph with vertex set \([v]\). The
additional requirement is that each vertex must appear in the same number of these complete subgraphs, so using a triangle and three edges in $K_4$ does not qualify.

A special construction uses the octahedron graph, the 4-regular planar triangulation on six vertices. The edge set decomposes into four triangles, with each vertex appearing in two of them. The complement of the octahedron is $3K_2$, so the remaining pairs are covered by three blocks of size 2, with each vertex appearing in one of them. We have created a 6-element design in which each element appears in two blocks of size 3 and one block of size 2.

The idea of leaving a regular complement leads to a simple infinite family. When $p$ divides $v$, we can use $v/p$ disjoint copies of $K_p$ and cover the remaining pairs with $v(v-p)/2$ copies of $K_2$. Each vertex appears in one block of size $p$ and $v-p$ blocks of size $2$.

13.1.6. For $n \in \mathbb{N}$ and $1 \leq k \leq n-1$, entry $(i, j)$ of the $n$-by-$n$ matrix $A^{(k)}$ is the congruence class of $ki+j$ modulo $n$.

a) $A^{(k)}$ is a Latin square if and only if $n$ and $k$ are relatively prime. If $ki+j = ki'+j'$, then $j = j'$, so the rows always consist of $n$ distinct values. Row $n$ is always $1, \ldots, n$ in order. If $n$ and $k$ have a common divisor $d$ greater than 1, then row $n/d$ is the same as row $n$.

If $n$ and $k$ are relatively prime, then there exists $t \in [n-1]$ such that $kt \equiv 1 \pmod{n}$. If $ki+j = ki'+j$, then $ki = ki'$, and multiplying by $t$ yields $i \equiv i' \pmod{n}$. Since $i, i' \in [n]$, we have $i = i'$. Thus, the columns also consist of $n$ distinct entries.

b) If $A^{(k)}$ and $A^{(l)}$ are Latin squares, then they are orthogonal if and only if $k-l$ is relatively prime to $n$. Suppose that the two squares have the same ordered pair of elements in positions $(i, j)$ and $(r, s)$. Thus $ki+j = kr+s$ and $li+j = lr+s$. Subtracting the equations yields $(k-l)i = (k-l)r$. If $k-l$ is relatively prime to $n$, then there exists $t$ such that $(k-l)t \equiv 1 \pmod{n}$. Multiplying the equation by $t$ yields $i \equiv r \pmod{n}$. Since $i, r \in [n]$, we conclude that $i = r$. This immediately yields $j = s$. Hence the two squares cannot have the same ordered pairs in two positions.

Squares $A^{(k)}$ and $A^{(l)}$ both have $1, \ldots, n$ as the last row. Hence the ordered pairs $(i, i)$ occur in that row. If $k-l$ and $n$ have a common divisor $d$ greater than 1, then the difference between $k(n/d)+j$ and $l(n/d)+j$ is $n(k-l)/d$, which is a multiple of $n$. Hence row $n/d$ is the same in both squares, and the pairs $(i, i)$ occur again, violating orthogonality.

c) This construction generates no larger family of pairwise orthogonal Latin squares of order $n$ than the Moore-MacNeish construction does from the prime factorization. The size of the Moore-MacNeish family is $q - 1$, where $q$ is the smallest of $p_1^e, \ldots, p_k^e$ in the factorization $n = \prod_{i=1}^{k} p_i^{e_i}$ into prime powers. Let $p = \min\{p_1, \ldots, p_k\}$. In the construction above, we cannot choose $k$ and $l$ from the same congruence class modulo $p$, and we cannot choose a multiple of $p$. Hence at most $p - 1$ squares can be generated. Since $p - 1 \leq q - 1$, the result follows.

13.1.7. Transversals and orthogonal Latin squares. A transversal of a Latin square is a set of positions, one in each row and column, containing distinct elements.

a) A Latin square of order $n$ belongs to a pair of orthogonal Latin squares if and only if it consists of $n$ disjoint transversals. For necessity, let $A$ and $B$ be orthogonal Latin squares. The positions corresponding to a fixed label in $A$ from a transversal in $B$, and vice versa.

For sufficiency, given such a set of $n$ transversals in a Latin square $A$, form $B$ by using, for each of the $n$ transversals in $A$, one label in the corresponding positions for $B$. This uses $n$ labels in $B$, with each occurring once in each row and column. Hence $B$ is a Latin square, and it is orthogonal to $A$.

b) No Latin square is orthogonal to the Latin square below.

$$
\begin{pmatrix}
 a & b & c & d \\
 b & d & a & c \\
 c & a & d & b \\
 d & c & b & a
\end{pmatrix}
$$

It suffices to show that the square does not decompose into transversals. In fact, there is no transversal containing the element $a$ in the upper left corner. The remaining three elements must come from the elements other than $a$ in the lower left matrix of order 3; they must be distinct labels and have no two in the same row and column. However, the only such sets of three positions contain labels $(d, b, b)$ or $(d, c, c)$.

13.1.8. Let $M$ be a Latin square that can be written as a block matrix $(X Y \ X)$, where $X$ and $Y$ are Latin squares of odd order.

$M$ has no transversal. Let $X$ and $Y$ have order $l$. A transversal must use $l$ positions in every set of $l$ rows or $l$ columns. It must also use $l$ labels from $X$ and $l$ labels from $Y$, since those are the only labels available. Hence if $a, b, c, d$ are the number of labels used from the four quadrants of $M$, respectively, then every two among $a, b, c, d$ must sum to $l$. In particular, they must all equal $l/2$, which is impossible when $l$ is odd.

No Latin square is orthogonal to $M$. Suppose that $L$ is orthogonal to $M$. Any label in $L$ appears once in each row and column. By orthogonality, the corresponding positions in $M$ have distinct elements. Hence they form a transversal, which we showed is impossible.

13.1.9. There is a Latin square of order $n$ where each row is a rotation of
the first and the main diagonal consists of 1, \ldots, n in order if and only if $n$ is odd. Let the elements be $[n]$. A Latin square describes a binary relation called a “quasigroup”; the property of the diagonal requested here is idempotence. The full square is determined by the first row and idempotence. Given the first row, moving the value $k$ to become the diagonal element in row $i$ specifies the amount of rotation. The rotations of the first row will form a Latin square if and only if the amounts of rotation are distinct. The problem is thus to find a permutation $\sigma$ of $[n]$ as the first row so that the amounts of rotation forced by idempotence are distinct.

Row $k$ has $k$ in column $k$. If $\sigma = \sigma(j)$, then $\sigma$ is rotated leftward $j - k$ positions (modulo $n$) to become row $k$. Thus the values $\sigma^{-1}(k) - k$ must be distinct for $k \in [n]$.

When $n$ is odd, let $\sigma = (1, (n+3)/2, 2, (n+5)/2, \ldots, (n+1)/2)$. Moving $k$ to position $k$ requires rotating leftward $k - 1$ positions. Thus resulting amounts of rotation for the rows are distinct, so they produce a Latin square with the desired diagonal.

If the values $\sigma^{-1}(k) - k$ are distinct (modulo $n$), then their sum is congruent to $\sum_{i=1}^{n} i$, which equals $(n+1)n/2$. When $n$ is even, this is congruent to $n/2$ modulo $n$. However, the fact that the values in $\sigma^{-1}$ are all values in $[n]$ implies that the sum must be 0.

13.1.10. Existence of MOLS($n, n-2$) implies existence of MOLS($n, n-1$). Let $A_1, \ldots, A_{n-2}$ be pairwise orthogonal Latin squares of order $n$, all normalized by renaming elements to have first row 1 through $n$ in order. We construct $A_{n-1}$.

First let $A_{n-1}$ also have first row 1 through $n$. The pairs $(j, j)$ occur in the first row when pairing $A_{n-1}$ with any other square in the set. Now there is only one choice for each entry below the first row, since the entry in such position $(i, j)$ must differ from $j$ and from the entries in position $(i, j)$ of the other matrices. Those entries are distinct, since the pairs of those matrices also have $(j, j)$ in the first row, and they also differ from $j$ at the top of the column. Hence $n - 1$ values are forbidden from each position.

We claim that the resulting matrix is a Latin square and is orthogonal to the others. Since there are $n - 2$ other squares, each having $j$ somewhere in row $i$, each element $j$ is forbidden from $n - 2$ positions in row $i$, and separately also from column $j$. Hence each element is forbidden from $n - 1$ positions in row $i$. Since for each position there is a element not forbidden, those elements must be distinct. The analogous argument applies to the elements other than $j$ in the $j$th column.

To prove orthogonality with an earlier matrix $A_\tau$, let $S$ be the set of positions in $A_\tau$ containing element $j$. It suffices to show that in $A_{n-1}$ the positions $S$ have distinct values. Because $A_\tau$ is orthogonal to the others among the first $n - 2$, these positions form transversals in each of those matrices. They all have $j$ in the first row, so the occurrences of values other than $j$ are in distinct positions in $S$ in these matrices, and the occurrences of entry $k$ in $S$ are not in column $k$. Hence each entry $k$ has already been forbidden from $n - 2$ positions in $S$ below the first row. Since we found allowable values for each position in $A_{n-1}$, the positions in $S$ allowed for the various values of $k$ must be distinct, as desired.

13.1.11. Existence of MOLS($n, k$) implies existence of $k - 1$ pairwise orthogonal Latin squares whose diagonals are transversals. Simultaneous column permutations can be performed to bring element 1 to the diagonal in each column of the first square. The transformed squares are still pairwise orthogonal. Now orthogonality requires the diagonal in each of the squares other than the first to be a transversal. By permuting the names of elements in those squares, one can make each of those diagonals be 1 through $n$ in order.

13.1.12. If $S$ is a set of $k$ elements in a symmetric $(v, k, \lambda)$-design, and $S$ intersects each block at least $\lambda$ times, then $S$ is a block.

Since the design is symmetric, there are $v$ blocks, and each elements appears in $k$ blocks. Let $x_1, \ldots, x_v$ be the sizes of the intersections of $S$ with the various blocks; by hypothesis, $x_i \geq \lambda$ for each $i$.

The total number of appearances of elements of $S$ is $\sum x_i$, but it also must equal $r |S|$; thus $\sum x_i = k^2 = k + k(k - 1) = k + \lambda(v - 1)$. Let $N$ be the total number of appearances of pairs of elements of $S$. We have $m = \sum (\binom{x_i}{2})$, but also $m$ must equal $\lambda \binom{|S|}{2}$.

Since $\sum x_i$ has fixed sum, we can make $\sum (\binom{x_i}{2})$ larger by increasing $x_i$ and decreasing $x_j$ by the same amount if $x_i \geq x_j$. Since we must keep each $x_i$ at least $\lambda$, we make $m$ largest by having all but one $x_i$ equal to $\lambda$ and the remaining value equal to the rest. Since $\sum x_i = k + \lambda(v - 1)$, the rest equals $k$. Using these values, $m = \binom{k}{2} + (v - 1)\binom{\lambda}{2} = \binom{k}{2} + k(k - 1)\frac{\lambda}{2} = \lambda \frac{\binom{|S|}{2}}{2}$. Hence the only way to obtain the required number of appearances of pairs of elements of $S$ is if $S$ completely overlaps with one block.

13.1.13. If $A$ is a matrix of order $n$ whose entries are real and have absolute value at most 1, then $|\det A| \leq n^n/2$, with equality only when $A$ is a Hadamard matrix. The absolute value of determinant of an $n$-by-$n$ matrix is the $n$-dimensional volume of the parallelotope spanned by the rows. When the magnitudes of the row vectors are fixed, the volume is maximized by making the row vectors pairwise orthogonal. After that, it is maximized by making the row vectors as long as allowed, which under the given condition means making each entry $\pm 1$. These conditions now
specify a Hadamard matrix, for which the resulting volume is $\sqrt{n}$, since each row vector has length $\sqrt{n}$.

13.1.14. With $P(i, j, k, l) = \{s \in \mathbb{Z}_n^4\}$ such that $s_1 = k$ and $s_j = l$ for fixed distinct $i, j \in [4]$, there is a function $\phi: \mathbb{Z}_n^4 \rightarrow \mathbb{Z}_n^4$ that is surjective on each $P(i, j, k, l)$ if and only if there are two orthogonal Latin squares of order $n$.

Given orthogonal Latin squares $L_1$ and $L_2$ of order $n$, let

$$\phi(s) = (s_3 - L_1(s_1, s_2), s_4 - L_2(s_1, s_2)).$$

Consider a plane $P(i, j, k, l)$. If $\{i, j\} = \{3, 4\}$, then $s_3$ and $s_4$ are fixed, and the orthogonality of $L_1$ and $L_2$ yields $n^2$ distinct values of $\phi(s)$ on $P(i, j, k, l)$. If $\{i, j\} = \{1, 2\}$, then only one position in the squares is accessed, and again all $n^2$ values of $s$ are distinct. By symmetry, it remains only to consider $\{i, j\} = \{1, 3\}$. The choice of $s_3$ fixes one of the $n$ values in the first coordinate, and because $L_2(s_1, s_2)$ is now fixed, the choice of $s_4$ yields all $n$ pairs with that first coordinate.

Conversely, let $\phi$ be such a map. Each plane fixing two positions is mapped by $\phi$ to $n^2$ distinct values. Let $(s_1, s_2, p, q)$ be the point in the plane $P(1, 2, s_1, s_2)$ that is mapped by $\phi$ to $(0, 0)$. Set $L_1(s_1, s_2) = p$ and $L_2(s_1, s_2) = q$. Since two points agreeing in two positions cannot both be mapped by $\phi$ to $(0, 0)$, the entries in a fixed row or column of $L_1$ or $L_2$ are distinct, and the Latin squares $L_1$ and $L_2$ are orthogonal.

13.1.15. $K_{7,7}$ is not 3-choosable. Let the parts of $K_{7,7}$ be $X$ and $Y$. We provide a 3-uniform list assignment $L$ from which no proper coloring can be chosen. Assign as lists to each part the seven triples in $[7]$ that are lines in the Fano plane.

Consider an $L$-coloring $f$; all colors used lie in $[7]$. By symmetry, we may assume that $f$ uses at most three colors on $X$. If only two colors are used on $X$, then they appear together in one line and miss any other line containing the third point of the line, since lines intersect once.

Hence exactly three colors are used on $X$; let $C$ be this set of colors. If $[7] - C$ contains a line, then no color was chosen from that line in $X$. Since lines have the form $(i, i + 1, i + 3)$, we conclude that $C$ cannot have any of the forms $(i, j + 1, j + 2), (i, j + 2, j + 3), (i, j + 2, j + 4), (i, j + 3, j + 4)$. The remaining type is $(j, j + 1, j + 3)$, which is a line. In this case no color can be chosen for the vertex of $Y$ whose list is $C$.

13.1.16. There is a Hadamard matrix of order $4m$ if and only if there is a $(4m - 1, 2m, m)$-design. Since $r(k - 1) = \lambda v(1 - 1)$, each element in a $(4m - 1, 2m, m)$-design appears in $m(4m - 2)/(2m - 1)$ block; that is, $r = 2m$. Also $bk = vr$, so the number of blocks is $(4m - 1)(2m)/(2m)$, which equals $4m - 1$. Thus the incidence matrix of the design is a square matrix $A$ of order $4m - 1$ with $2m$ positions having 1 in each column and each row.

Furthermore, since $\lambda = m$, any two rows have 1 in $m$ common columns. Since there are $2m$ positions with 1 in each row, canceling the positions where both have 1 yields $2m$ columns where the rows differ.

Form $H$ from $A$ by changing each 1 to $-1$ and each 0 to 1, and add a first row and column with 1 in each position. We claim that $H$ is a normalized Hadamard matrix. All entries are $\pm 1$. Since any two rows differ in $2m$ columns (including the first new row), and hence they agree in $2m$ columns, the dot product of any two rows is 0, as desired.

Given a Hadamard matrix of order $4m$, the transformation can be reversed after normalizing the first row and column. This proves the converse.

13.1.17. The minimum number of functions in a $[k]$-pair-covering of $G$ is $k^2$ if and only if there exists a family of $n - 2$ pairwise orthogonal Latin squares of order $k$. A $[k]$-pair-covering of a graph $G$ is a list of functions $f_1, \ldots, f_m$ with $f_i: V(G) \rightarrow [k]$ such that for every edge $uv$ and every ordered pair $(r, s) \in [k]^2$, there is some $t$ such that $f_i(u) = r$ and $f_i(v) = s$.

Since the functions must yield $k^2$ ordered pairs of images on $u$ and $v$ when $u \leftrightarrow v$, there must be at least $k^2$ functions. Suppose there is such a covering by functions $f_1, \ldots, f_{k^2}$, and choose two special vertices $u$ and $v$. We form a Latin square for each of the other vertices. For the vertex $x$, let the value in position $(i, j)$ be $f_i(x)$, where $f_i$ is the function in the covering such that $f_i(u) = i$ and $f_i(v) = j$. Let $l = f_r(x)$. Since the pairs $(i, l)$ and $(j, l)$ occur only once on $(u, x)$ and $(v, x)$, each of the $n - 2$ matrices constructed is a Latin square. To show that they are pairwise orthogonal, suppose that position $(i, j)$ exhibits the elements $r$ and $s$ in two squares $x$ and $y$, and some other position also exhibits this pair. This cannot happen, because it requires the edge $xy$ to have the ordered pair $(r, s)$ in the function where $uv$ has $(i, j)$. Since $(r, s)$ occurs on $xy$ only once in the covering, it cannot also occur in the function where $uv$ has some pair (position) other than $(i, j)$.

For the converse, we reverse the construction. Associate the $n - 2$ squares with the vertices other than $u$ and $v$. Define the function $f_i$ by setting $f_i(u) = i, f_i(v) = j$, and $f_i(x)$ to the value in position $(i, j)$ of square $x$. By construction, the pairs on $(i, j)$ are distinct. Since square $x$ is a Latin square, the pairs on $(u, x)$ (from the labels in row $i$ of square $x$) are distinct, and the pairs on $(v, x)$ (from the labels in column $j$ of square $x$) are distinct. For the edge $xy$, the ordered pairs distinct because they are the pairs from corresponding positions of square $x$ and square $y$, and these two Latin squares are orthogonal.

13.1.18. The product dimension of $nK_m$ is $m$ if and only if there is a family of $(n - 1)$ pairwise orthogonal Latin squares of order $m$. 
Chapter 13: Combinatorial Designs

The product dimension is the minimum $t$ such that vertices can be coded as $t$-tuples such that vertices are adjacent if and only their codes differ in every coordinate. Let $H_k$ be the $k$th component of $nK_m$, and let $v_r^i$ be the $i$th vertex in $H_k$. We treat the code assigned to $v_r^i$ as $v_r^i$ itself.

Note that the product dimension of $nK_m$ is always at least $m$ when $n \geq 2$. Consider $H_k$ and a vertex $v$ outside it. This vertex must agree with each vertex in $H_k$ in at least one position. However, no two vertices in $H_k$ agree in any position. Hence $v$ must agree with the $m$ vertices in $H_k$ in distinct coordinates. Hence there are at least $m$ coordinates. We prove that equality holds if and only if the specified family exists.

**Necessity.** We are given a product representation of $nK_m$ with $m$ coordinates. Vertices in $H_k$ and $H_l$ must agree in some coordinate. Since the values in coordinate $j$ for the vertices within one component are distinct, each vertex in $H_k$ can only agree with one vertex in $H_l$ in each coordinate. It must agree somewhere with each vertex in $H_l$, so each vertex in $H_k$ agrees in exactly one coordinate with each vertex in $H_l$, and each coordinate of each vertex in $H_k$ gives one such agreement.

For $1 \leq k \leq n - 1$, define $A(k)$ by comparing $H_k$ with $H_n$. Let $j$ be the unique coordinate where $v_r^i$ agrees with $v_r^j$; place $i$ in column $j$ in row $r$ of $A(k)$. By the remarks above, this places $i$ in each row and only once in each column, for $1 \leq i \leq m$, so $A(k)$ is a Latin square.

For orthogonality, consider $i, i' \in [m]$ and $k \neq l$. Let $j$ be the unique coordinate where $v_r^i$ agrees with $v_r^{i'}$. This coordinate also agrees with one vertex $v_r^j$ of $H_n$ in position $j$. Hence $(i, i')$ appears in position $(r, j)$ of $A(k)$ and $A(l)$. Since each of the $m^2$ pairs of labels appears in some corresponding position in the two squares, the squares are orthogonal.

** Sufficiency.** Let $A(1) \ldots A(n - 1)$ be a family of pairwise orthogonal Latin squares of order $n$. We use $[m]$ as the set of labels in each $A(k)$. We produce an encoding of $nK_m$ by integer $m$-tuples. This shows that the product dimension is at most $m$.

To reverse the construction above, we use $H_n$ as a reference clique. For $k = n$, let $v_r^i = (i, \ldots, i)$. To make each vertex outside $H_n$ agree in some coordinate with each vertex of $H_n$, all other vertices will be permutations of $[m]$. For $k = 1$, let $v_r^i$ be the $i$th row of $A(1)$. Since $A(1)$ is a Latin square, two such vertices differ in every coordinate and agree with every vertex of $H_n$ in some coordinate.

For $2 \leq k \leq n - 1$, we name $v_r^i$ using entries of $A(1)$ corresponding to the positions of label $i$ in $A(k)$. In particular, let coordinate $j$ for $v_r^i$ be $A_{r,j}^{(1)}$, where $i$ appears in row $r$ in column $j$ of $A(k)$.

Since $A(k)$ is orthogonal to $A(1)$, the values in $A(1)$ in the positions occupied by $i$ in $A(k)$ are distinct. Hence $v_r^i$ is a permutation of $[m]$, as desired to make $v_r^i$ nonadjacent to $H_n$. To conclude that $v_r^i$ and $v_r^j$ differ in position $j$, let $r$ and $r'$ be the rows occupied by $i$ and $j'$ in column $j$ of $A(k)$. We have $r \neq r'$, and hence $A_{r,j}^{(1)} \neq A_{r',j}^{(1)}$. Thus any two vertices in the same component $H_k$ differ in every component.

We must show that $v_r^i$ and $v_r^j$ agree in some coordinate, for $2 \leq k \leq n - 1$ and all $r, i \in [m]$. This holds because coordinate $j$ of $v_r^i$ goes to coordinate $j$ of $v_r^j$ when $i$ appears in row $r$ of column $j$ in $A(k)$. Since $i$ appears in every row of $A(k)$, for each $r$ we make $v_r^i$ agree with $v_r^j$ in some coordinate. Finally, it remains to show that $v_r^i$ and $v_r^j$ agree in some coordinate when $k < l$ and $i, i' \in [m]$. Since $A(k)$ and $A(l)$ are orthogonal, there is a unique position $(r, j)$ such that $A_{r,j}^{(k)} = i$ and $A_{r,j}^{(l)} = i'$. Now $v_r^i$ and $v_r^j$ both have $A_{r,j}^{(k)}$ in coordinate $j$.

13.1.19. Bipartite Ramsey. Define $b(2, t)$ as in Application 13.1.33. We seek the least $n$ such that every 2-edge-coloring of the $X, Y$-bigraph $K_{n,n}$ has a monochromatic copy of $K_{2,t}$, with the small part in $X$.

a) $b(2, t) \leq 4t - 3$. Consider a coloring with no such copy. Let red be the color on at least $n^2/2$ edges, and let $G$ be the red subgraph, with $m$ edges. Since no two vertices in $X$ can have $t$ common neighbors via red edges, and $(\binom{n}{2})$ is a convex function of $x$, we have

$$n \binom{n/2}{2} \leq \sum \binom{d(y)}{2} \leq (t - 1) \binom{n}{2}.$$

This simplifies to $n \frac{n - 2}{n - 1} \leq 4t - 4$, which requires $n \leq 4t - 3$ for integer $n$ and proves $b(2, t) \leq 4t - 2$. To improve the bound, we consider the lower bound on $\sum \binom{d(y)}{2}$ when $n = 4t - 3$. We have $\sum \binom{d(y)}{2} = m \geq \lceil n^2/2 \rceil$. Since $4t - 3$ is odd, $m \geq (n^2 + 3)/2$.

We still use the lower bound from letting the degrees be equal; the inequality is now $(n + 3)/n(n - 2 + 3/n) \leq (4t - 4)(n - 1)$. Letting $n = 4t - 3$ and $N = 4t - 4$, the inequality becomes $N^2 \geq (N + 3 + 3/n)(N - 1 + 3/n) = N^2 - 1 + 6N/n + 9/n^2$. Since $6(n - 1)/n > 1$ when $n > 6/5$, the inequality cannot hold, so when $n = 4t - 3$ the monochromatic copy occurs, and $b(2, t) \leq 4t - 3$.

b) $b(2, t) \geq 4t - 4$ when a Hadamard matrix of order $4t - 4$ exists. Normalize the Hadamard matrix and delete the first row and column, yielding a matrix of order $4t - 5$. The sign pattern provides a 2-coloring of $E(K_{4t-5, 4t-5})$, with $X$ corresponding to rows and $Y$ corresponding to columns. Every two rows have exactly $t - 1$ columns with common 1s and $t - 1$ columns with common −1s; in the remaining $2t - 3$ columns the entries in the two rows differ. Thus every two vertices in $X$ lie in $K_{2, t - 1}$ in each color, but there is no monochromatic $K_{2, t}$, so $b(2, t) > 4t - 5$. 


13.1.20. If $C$ is a symmetric conference matrix of order $n$, then $H$ is a Hadamard matrix of order $2n$, where $H = (C + I)C - I$. It suffices to prove $HH^T = 2nI'$, where $I'$ is the identity matrix of order $2n$, and $I$ in the block definition of $H$ is the identity matrix of order $n$. Note that $CC^T = (n - 1)I$ and $C^T - C = 0$. Using block multiplications, we compute

$$HH^T = \begin{pmatrix} C + I & C - I \\ C - I & -C - I \end{pmatrix} \begin{pmatrix} C^T + I & C^T - I \\ C^T - I & -C^T - I \end{pmatrix} = \begin{pmatrix} (C + I)(C^T + I) + (C - I)(C^T - I) & (C + I)(C^T - I) - (C - I)(C^T + I) \\ (C - I)(C^T + I) - (C + I)(C^T - I) & (C - I)(C^T - I) + (C + I)(C^T + I) \end{pmatrix}$$

$$= \begin{pmatrix} CC^T + C^T + C + I + CC^T - C^T - C + I & CC^T + C^T - C - I - CC^T + CT^T + C^T - C + I \\ CC^T - C^T + C - I - CC^T - C^T + C + I & CC^T - C^T - C + I + CC^T + CT^T + C^T + C + I \end{pmatrix}$$

$$= \begin{pmatrix} 2CC^T + 2I & 2(C^T - C) \\ 2(n - 1)I + 2I & 0 \end{pmatrix} = 2nI'.$$

13.2. PROJECTIVE PLANES

13.2.1. Uniqueness of the Fano plane. Consider a projective plane of order 2, with seven points and seven lines. Name the points in one line $L$ as $\{1, 2, 4\}$. Take another point, 3. This point 3 determines distinct lines with each of the points in $L$, since no two of them can appear together in another line. Let these lines be $23x$, $34y$, and $31z$. We may label these elements so that $x = 5$, $y = 6$, and $z = 7$.

Finally, we show that the remaining three lines are determined as in the Fano plane. Each of $\{1, 2, 4\}$ has appeared in two lines but with only one of $\{5, 6, 7\}$. Hence each of the remaining three lines must consist of one of $\{1, 2, 4\}$ and the appropriate two among $\{5, 6, 7\}$; they are $561$, $672$, and $457$.

13.2.2. The Heawood graph is the incidence bigraph of the Fano plane. Labeling vertices by the points and lines, adjacency corresponds to membership of points in lines.

13.2.3. $\{1, 2, 5, 15, 17\}$ is a $(21, 5, 1)$-difference set. It suffices to find the differences 1 through 10, since subtracting in the other order yields their negatives. We have $2 - 1 = 1$, $17 - 15 = 2$, $5 - 2 = 3$, $5 - 1 = 4$, $1 - 17 = 5$, $2 - 17 = 6$, $15 - 5 = 10$, and $2 - 15 = 7$. Hence each of the remaining three lines must consist of $\{1, 2, 5, 15, 17\}$ and the appropriate two among $\{6, 7\}$; they are $671$, $713$, and $124$.

The Heawood graph is the incidence bigraph of the Fano plane. Labeling vertices by the points and lines, adjacency corresponds to membership of points in lines.
that positions \((i, j)\) and \((r, s)\) are independent if \(i \neq r\) and \(j \neq s\). It suffices to show that in a complete family, any two independent positions contain the same value in exactly one square.

In a given square, a given value occurs \(q\) times in independent positions, generating \(\binom{q}{2}\) pairs of independent positions with the same value. This occurs over \(q^2\) values and \(q - 1\) squares, so in total there are \(q^2(q-1)^2/2\) such pairs. This is precisely the number of pairs of independent positions. If any pair of independent positions has the same value twice, say \(A_{i,j}^{(k)} = A_{r,s}^{(k)}\) and \(A_{i,j}^{(k')} = A_{r,s}^{(k')}\), then the pairs \((A_{i,j}^{(k)}, A_{i,j}^{(k')})\) and \((A_{r,s}^{(k)}, A_{r,s}^{(k')})\) are the same, contradicting orthogonality of \(A^{(k)}\) and \(A^{(k')}\). Hence every pair \((i, j)\) and \((r, s)\) of independent positions occurs with the same value exactly once, determining a unique line containing \(z_{i,j}\) and \(z_{r,s}\).

We have proved that every two points appear together in one common line. This immediately implies that every two lines have at most one common point. The number of occurrence of a point on two lines is \((q+1)^2/2\) for each point, altogether \((q^2+q+1)(q+1)/2\) over all points. The number of pairs of lines is \((q^2+q+1)^2/2\), which has the same value. Since no two lines have two common points, each pair of lines appears in the set of pairs having one common point.

**13.2.5. The hypergraph of a projective plane of order \(q\) is \(2\)-colorable if and only if \(q > 2\).** If \(q > 2\), then lines have size at least 4. Let \(x, y, z\) be three points not on a line (these exists since there are four points with no three on a line). These three points determine, in pairs, three lines \(A, B, C\). Give color red to the points on \(A \cup B \cup C\) outside of \((x, y, z)\). Give color blue to \(x, y, z\) and to the points not on \(A \cup B \cup C\).

This \(2\)-coloring is proper. We used two colors on \(A, B, C\). Other lines contain at most one of \((x, y, z)\). If none, then their three points in \(A \cup B \cup C\) are red, and their points outside \(A \cup B \cup C\) are blue (and this set is nonempty since \(q > 2\)). In the other case, by symmetry we may assume that \(x \in L\) and \((x) = A \cap B\). Now \(x\) is blue and \(L\) has a red point in \(C\).

In a \(2\)-coloring of the Fano plane (the case \(q = 2\)), some color must appear on at most three points; let \(S\) be this set of at most three points. If \(S\) forms an edge, then the coloring is not proper.

Otherwise, \(S\) is incident to at most six edges, since any set of four points in the Fano plane that is not the complement of a line contains a line (consider congruence classes modulo 7). The leftover edge is monochromatic in the other color.

**13.2.6. Transversal numbers of hypergraphs.** Let \(H\) be the hypergraph with \(q^2 + q + 1\) vertices whose edges are the lines of a projective plane of order \(q\). Let \(H'\) be the hypergraph with the same vertex set whose edges are the complements of the edges in \(H\). The transversal number is the minimum size of a set of vertices that intersects every edge.

The transversal number of \(H\) is \(q + 1\). Since every two lines in the plane have one common point, the set of vertices in any one edge of \(H\) contains exactly one vertex from every other edge of \(H\). Any set of \(q\) vertices each appear in \(q + 1\) lines and hence together can intersect at most \(q(q+1)\) of the \(q^2 + q + 1\) edges of \(H\).

The transversal number of \(H'\) is 3. Any two vertices appear together in exactly one line and hence are both omitted by the complement of exactly one edge of \(H\). Adding one vertex from that complement completes a transversal of \(H'\).

**13.2.7. When \(q\) is a prime power congruent to 0 or 1 modulo 4, the number of nonzero multiplicative classes of solutions to \(a^2 + b^2 + c^2 = 0\) is \(q + 1\).** It suffices to show that the total number of solutions is \(q^2\), since we then delete the all-0 solution and divide by \(q - 1\), the size of a nonzero multiplicative class.

When \(q\) is a power of 2, we have \(a^2 + b^2 + c^2 = (a+b+c)^2\), so we require \(a + b + c = 0\). There is one solution for each choice of \((a, b)\).

When \(q \equiv 1 \pmod{4}\), there exists \(j \in \mathbb{F}_q\) with \(j^2 = -1\). Let \(u = a + j b\) and \(v = a - j b\), so \(a = (u + v)/2\) and \(b = (w/v)/2j\). Now we seek solutions to \(uv = -c^2\). For \(c = 0\) there are \(2q - 1\) solutions; \(u\) or \(v\) must be 0. For each of the \(q - 1\) nonzero values of \(c\) there are \(q - 1\) solutions, since \(\mathbb{F}_q - \{0\}\) is a multiplicative group. Altogether, the number of solutions is \((2q - 1) + (q - 1)^2\), which equals \(q^2\).

**13.2.8. Solutions to \(a^2 + b^2 + c^2 = 0\) when \(q\) is a prime power congruent to 3 modulo 4.** Let \(S_0\) and \(S_1\) be the set of nonzero squares and the set of nonsquares in \(\mathbb{F}_q\). Note that \(-1 \in S_1\), and hence \(x \in S_0\) if and only if \(-x \in S_1\) for \(x \neq 0\). For \(i, j \in \{0, 1\}\), let \(T_{i,j} = \{x \in S_i; x + 1 \in S_j\}\), and \(T_{i,j} = |T_{i,j}|\).

\(a)\) \(t_{0,0} = t_{1,0} = t_{1,1} = (q - 3)/4\) and \(t_{0,1} = (q + 1)/4\). Note \(t_{0,0} - t_{0,1} = S_0 \cup S_1, T_{0,0} = T_{0,1}, T_{0,1} = T_{1,0}, S_1 = (q-1)/2\). Since also \(|S_0| = |S_1| = (q-1)/2\), we have \(t_{0,0} + t_{0,1} = (q-1)/2\) and \(t_{1,0} + t_{1,1} = (q-3)/2\). Also, \(S_1\) consists of all elements obtained by adding 1 to elements of \(T_{0,1} \cup T_{1,1}\), so \(t_{0,1} + t_{1,1} = (q - 1)/2\).

It now suffices to show \(t_{1,0} = t_{0,0}\); we then have four equations in four unknowns, and the unique solution is as claimed above. To prove this, consider the bijection on \(\mathbb{F}_q - \{0\}\) that maps \(x\) to \(1/x\). If \(x \in T_{1,0}\), then \(x\) is not a square and \(x + 1\) is a square. Also \(1/x\) is not a square, and \((1/x) + 1\) equals \(-x\). Since \(x + 1\) is a square and \(x\) is not, \(-x\) is a square. Hence \(T_{1,0}\) is mapped into \(T_{1,1}\). Furthermore, the argument is reversible: that is, \(x \in T_{1,0}\) if and only if \(1/x \in T_{1,1}\), and hence \(t_{1,0} = t_{1,1}\).

Comment: Similar arguments when \(q \equiv 1 \pmod{4}\) yield \(t_{0,1} = t_{1,0} =\)
$t_{1,1} = (q - 1)/4$ and $t_{0,0} = (q - 5)/4$ in that case.

b) The number of multiplicative classes of nonzero triples solving $a^2 + b^2 + c^2 = 0$ is $q + 1$. For each class, take the member $(a, b, c)$ whose first nonzero coordinate is 1. If $a = 0$, then $b^2 = -c^2$, which is solvable only by $(0, 0)$ since $-1$ is not a square. Hence we may assume $a = 1$.

For $x \in T_{0,1}$, the four triples $(1, \pm \sqrt{x}, \pm \sqrt{-x - 1})$ are solutions, where the square root sign indicates one of the two square roots of a square. We have chosen $x \in S_0$ so that $x + 1 \in S_1$; since exactly one of $\{z, -z\}$ is a square when $q \equiv 3 \pmod{4}$ and $z \neq 0$, we have $-x - 1 \in S_0$.

Conversely, this describes all solutions. Just as we eliminated $a = 0$, also $b, c \neq 0$ in our equation $1 + b^2 + c^2 = 0$. Setting $x = b^2$ thus requires $b = \pm \sqrt{x}$ with $x \in S_0$, and $c^2 = -x - 1$, so $c = \pm \sqrt{1 - x}$ with $x \in S_1$.

Comment: The corresponding argument when $q \equiv 1 \pmod{4}$ yields triples $(0, 1, \pm \sqrt{-1})$, $(1, 0, \pm \sqrt{-1})$ and $(1, \pm \sqrt{-1}, 0)$, having a zero coordinate, plus those of the form $(1, \pm \sqrt{x}, \pm \sqrt{-x - 1})$ for $x \in T_{0,0}$. Since $t_{0,0} = (q - 5)/4$, again the number of solutions is $q + 1$.

When $q$ is a power of 2, the representative triples are $(0, 1, 1)$ and all $(1, x, x + 1)$ with $x \in \mathbb{F}_q$, since always $z + z = 0$ (that is, $1^2 + x^2 + (x + 1)^2 = 2 + 2x^2 = 0$).

13.2.9. The domination number of the incidence graph of a projective plane of order $q$ is 2q.

Lower bound. This graph $H$ is bipartite and $(q + 1)$-regular, with $q^2 + q + 1$ vertices in each part. If a dominating set $S$ contains at most $q - 1$ vertices in one part, then they dominate at most $q^2 - 1$ vertices in the other part. This implies that $S$ contains at least the remaining $q + 2$ vertices in the other part, yielding $|S| > 2q$. Hence the domination number exceeds 2q unless there is a dominating set with exactly $q$ vertices in each part.

Upper bound. Let $L$ be a line in the plane containing the point $x$. Let $S$ consist of all $q$ lines containing $x$ other than $L$, plus all $q$ points of $L$ other than $x$. Any line $L'$ not in $S$ shares one point with $L$, and that point is not $x$, so $L'$ is dominated by $S$. Any point $x'$ not in $S$ lies on a common line with $x$, and that line is not $L$, so $x'$ is dominated by $S$. Thus $S$ is a dominating set of size 2q.

13.2.10. Zarankiewicz problem for forbidden $K_{2,t}$. Let $G$ be an $n$-vertex graph with $m$ edges.

a) If $G$ is simple and $\sum_{v \in V} \binom{d(v)}{2} > (t - 1)\binom{n}{2}$, then $G$ contains $K_{2,t}$. If any two vertices have $t$ common neighbors, then $G$ contains $K_{2,t}$. With $\binom{q}{2}$ vertex pairs, a graph avoiding $K_{2,t}$ has at most $(t - 1)\binom{n}{2}$ choices of $x$, so by Sperner’s theorem, there are exactly $\sum_{v \in V} \binom{d(v)}{2}$ of them, which completes the proof.

b) $\sum_{v \in V} \binom{d(v)}{2} \geq m(2m/n - 1)$. Because $\binom{q}{2}$ is a convex function of $x$, $(\binom{q}{2}) + (\binom{q}{2}) \geq 2(\binom{q}{2})/2$. Hence $\sum_{v \in V} \binom{d(v)}{2}$ is minimized for fixed degree sum (number of edges) by setting all $d(v) = \sum d(v)/n = 2m/n$ (viewing $\binom{q}{2}$ as a polynomial in $x$), in which case the sum is $m(2m/n - 1)$.

c) If $m > \frac{1}{2}(t - 1)\binom{n}{2} + \frac{1}{4}n$, then $K_{2,t} \subseteq G$. The inequality implies $2m/n - 1 > (t - 1)\binom{n}{2} - \frac{1}{2}t$, so obtain $m(2m/n - 1) > \frac{1}{2}(t - 1)n^2 - n/8$. By (b), we obtain the hypothesis of (a), so $K_{2,t} \subseteq G$.

d) Among $n$ points in the plane, at most $n^{3/2}/\sqrt{2} + n/4$ pairs have distance exactly 1. Form a graph $G$ with vertices for the points and edges for pairs at distance 1. If $G$ has more edges than the specified number, then by (c) it contains $K_{2,3}$. However, no two points in the plane have distance exactly 1 from three other points, because the only point equidistant from three other points is the center of the circle through them.

13.2.11. Projective planes and graphs of girth 6.

a) Every $k$-regular graph of girth at least 6 has at least $2k^2 - 2k + 2$ vertices. If the girth of a graph is 6, then for every edge $uv$, there is at most one way to reach a vertex outside $\{u, v\}$ from $\{u, v\}$ in at most two steps. That is, the $2k - 2$ edges leaving $\{u, v\}$ reach distinct vertices, and each of these vertices has $k - 1$ additional neighbors that are neighbors of only one such vertex. This counting generates $2 + (2k - 2) + (2k - 2)(k - 1)$ distinct vertices, which yields the desired formula. Note that if the girth exceeds 6, even more vertices are required.

b) For $k \geq 3$, there is a $k$-regular graph of girth 6 with $2k^2 - 2k + 2$ vertices if and only if there is a projective plane of order $k - 1$.

Necessity. Let $G$ be such a graph. We first show that $G$ is bipartite. In the argument of part (a), the $2k^2 - 2k + 2$ vertices are all within distance 3 of both $u$ and $v$. Since the edge $uv$ was chosen arbitrarily, $G$ has diameter 3. Because $G$ has girth 6, the vertices at distance 2 from a given vertex form an independent set. As grown from the edge $uv$, the vertices at distance 3 from $u$ have distance 2 from $v$, and hence they also form an independent set. Now parity of the distance from $u$ defines a bipartition of $G$. Since $G$ is regular, the partite sets have the same size.
Sufficiency. Given a projective plane of order $k - 1$, the point/line incidence bigraph is a graph with the desired properties. It is bipartite and has no 4-cycles, so its girth is at least 6. It has $2k^2 - 2k + 2$ vertices, since there are $k^2 - k + 1$ points and the same number of lines, and hence it has girth exactly 6, by part (a).

13.2.12. There is no symmetric $(29, 8, 2)$-design. Note that $k(k - 1) = (v - 1)\lambda$, as is necessary. By the Bruck–Chowla–Ryser Theorem, existence requires an nonzero integer solution $(x, y, z)$ to $z^2 = 6x^2 + (-1)^{14}2y^2$. In a smallest solution, $\gcd(x, y, z) = 1$. In any solution, $z^2$ is even, so $z$ is even, so $4 | z^2$. Since 6 and 2 both are twice an odd number, $x^2$ and $y^2$ (and hence $x$ and $y$) have the same parity. Since there is no common factor, $x$ and $y$ are odd.

13.2.13. If $k, n \in \mathbb{N}$ and $\{G_1, \ldots, G_k\}$ is a decomposition of $K_n$, then

$$\sum_{i=1}^{k} \sigma(G_i) \leq \sqrt{k}n,$$

where $\sigma(G) = \max_{H \subseteq G} \delta(H)$. If $q = k^2 + 1$ for some prime power $q$, and $n \equiv 0 \pmod{k}$, then there is a decomposition $\{G_1, \ldots, G_k\}$ such that $\sum_{i=1}^{k} \sigma(G_i) \geq (\sqrt{k} - 1)n$.

Upper bound. Given a decomposition $\{G_1, \ldots, G_k\}$, let $d_i = \sigma(G_i)$ and $D = \sum_{i=1}^{k} d_i$. We prove $D \leq \sqrt{k}n$. Each $G_i$ has a subgraph $H_i$ such that $d_i = \delta(H_i)$. Thus $|E(G_i)| \geq |E(H_i)| \geq \binom{d_i}{2}$. Since $G_1, \ldots, G_k$ are edge-disjoint subgraphs of $K_n$, we obtain

$$n^2 \geq \binom{d_i}{2} \geq \frac{1}{2} \sum_{i=1}^{k} (d_i^2 + d_i) \geq \frac{1}{2} \left( \frac{D^2}{k} + D \right).$$

Consequently, $D^2 + kD - kn^2 \leq 0$, and thus $D \leq \frac{\sqrt{k}^2 n^2 - k}{4} \leq \sqrt{k}n$.

Construction. Let $q$ be a prime power, and let $k = q^2 + q + 1$ and $n = mk$ for some $m \in \mathbb{N}$. There is a projective plane with points $[k]$ and lines $\{g_1, \ldots, g_k\}$. Partition $V(K_n)$ into sets $X_1, \ldots, X_k$ of size $m$. Each line $g_i$ is a subset of $[k]$; let $H_i$ be the complete $(q+1)$-partite graph whose color classes are the elements of $\{X_1, \ldots, X_k\}$ indexed by $g_i$. The graphs $H_1, \ldots, H_k$ are edge-disjoint subgraphs of $K_n$, because in the projective plane any two points line on one common line. Thus there is a decomposition $\{G_1, \ldots, G_k\}$ of $K_n$ such that $H_i \subseteq G_i$ for each $i$ (the edges within $X_1, \ldots, X_k$ need to be added). Since $\sigma(G_i) \geq \delta(H_i) \geq qm$,

$$\sum_{i=1}^{k} \sigma(G_i) \geq kqm = qn \geq (\sqrt{k} - 1)n.$$

13.2.14. For prime power $q$ and $n = (q^2 - 1)/s$, construct an $n$-vertex graph $G$ with about $\frac{1}{2}\sqrt{s}n^{3/2}$ edges and no copy of $K_{2, s+1}$. We first define a relation on the nonzero ordered pairs of elements of $\mathbb{F}_q$. Since $s$ divides $q^2 - 1$, there is an element $\omega$ in $\mathbb{F}_q$ with multiplicative order $s$. The $s$ elements of $S = \{1, w, \ldots, w^{s-1}\}$ are distinct, and $w^s = 1$. Make $(a, b)$ equivalent to $(c, d)$ if $c = w^a$ and $d = w^b$ for some $i$.

This relation is an equivalence relation with equivalence classes all having size $s$. The relation is reflexive, since $(a, b) = w^0(a, b)$. It is symmetric, since the multiplicative inverse of $w^i$ is $w^{-i}$. It is transitive, since the product of powers of $w$ is a power of $w$. Given a nonzero pair $(a, b)$, by definition there are $s$ pairs satisfying the relation with $(a, b)$, so equivalence classes have size $s$.

The adjacency relation given by $(a, b) \leftrightarrow (u, v)$ if $au + bv \in S$, where $(a, b)$ denotes the class containing $(a, b)$, defines a graph having degrees $q$ or $q - 1$ and not containing $K_{2, s+1}$. By definition, the adjacency relation is symmetric. If $au + bv = w^i$, then $(w^a)u + (w^b)v = w^{i+1}$, so the relation is consistently defined for equivalence classes. That is, for a fixed pair $(a, b)$, the number of neighbors of $(a, b)$ in the graph is the number of solutions of $au + bv \in S$ divided by $s$.

For the pair $(0, b)$, there are $qs$ solutions; $u$ is arbitrary and then $v = w^a/b$. When $b$ is a power of $w$, the degree is only $q - 1$, since we do not allow loops. Similarly for $(a, 0)$. When both entries are nonzero, we may select $(1, b)$ from the class. Given a value $u$, we need $u + bv = w^i$. For each $i$, we compute $v = (w^i - u)/b$. This gives $qs$ solutions, with vertex degree again reduced from $q$ to $q - 1$ if $a^2 + b^2$ is a power of $w$.

Finally, consider the common neighbors of two classes $(a, b)$ and $(c, d)$. For such a pair $(a, b)$, both $au + bv$ and $cu + dv$ must be powers of $w$. Having specifies each of $(a, c, u)$, there are only $s^2$ allowable values for the pair $(au + bv, cu + dv)$. Hence there are at most $qs^2$ solution pairs for the two restrictions, which yields only $s$ classes as common neighbors.

13.2.15. Applications of the Multiplier Theorem.

a) A difference set that generates a projective plane of order 4. We seek a $(21, 5, 1)$-difference set. Since 2 divides 5 – 1 but not 21, the Multiplier Theorem implies that such a difference set, if it exists, can be formed as a union of orbits under multiplication by 2 modulo 21. The orbits are $\{0\}, \{1, 2, 4, 8, 16, 11\}, \{3, 6, 12\}, \{5, 10, 20, 19, 17, 13\}, \{7, 14\}$, and $\{9, 18, 15\}$. As verified below, the union $D = \{3, 6, 7, 12, 14\}$ is a $(21, 5, 1)$-difference set. We list the differences $1, \ldots, 10$ on the edges of the complete graph with vertex set $D$, and the remaining values are the differences between vertices in the other order.
b) A difference set that generates a projective plane of order 5. We seek a $(31, 6, 1)$-difference set. Since 5 divides $6 - 1$ but not 31, the Multiplier Theorem implies that such a difference set, if it exists, can be formed as a union of orbits under multiplication by 5 modulo 31. Since $5^3 = 125 \equiv 1 \pmod{31}$, the nonzero orbits have size at most 3; in fact, all have size 3. To shorten the computation, note that if $S$ is an orbit, then $-S$ is also an orbit.

$$\{1, 5, 25\} \cup \{2, 10, 19\} \cup \{3, 15, 13\} \cup \{4, 20, 7\} \cup \{8, 9, 14\} \cup \{20, 26, 6\} \cup \{29, 21, 12\} \cup \{28, 16, 18\} \cup \{27, 11, 24\} \cup \{23, 22, 17\}$$

A $(31, 6, 1)$-difference set (fixed under multiplication by 5 modulo 31) must be the union of two orbits. We focus on the differences 1 through 15. Each orbit gives three differences (and their negatives). Combining the two orbits gives nine more differences (and their negatives). When a pair misses a difference or has a repeated difference, it cannot combine to form a difference set (so an orbit and its negative can’t be used).

This leaves as many as 30 cases to test (two orbits from the first row, or an orbit from the first row with one from the second not directly below it). Most cases die quickly, and the problem ends as soon as one works. For example, $\{1, 5, 25\} \cup \{27, 11, 24\}$ is a suitable difference set. The first orbit gives differences $\{4, 11, 7\}$, the second gives $\{3, 13, 15\}$, and the cross differences are $\{5, 10, 8, 9, 6, 12, 2, 14, 1\}$ (grouped by the element from the first orbit).

13.2.16. (37,9,2) and (73,9,1).

13.2.17. No $(56,11,2)$.

13.2.18. $(n^2 + n + 1, n + 1, 1)$-difference set has multiplier $n$.

13.2.19. There is no $(111, 11, 1)$-difference set. Since $k - \lambda$ has factorization $2 \cdot 5$, and 111 is not divisible by 2 or 5, both 2 and 5 must be multipliers of every such difference set. If there is a difference set, then some translate of it is fixed by every multiplier.

Thus we may assume that 2 and 5 are multipliers of our difference set $D$. For each $x \in D$, this requires that $2x, 4x$, and $5x$ all belong to $D$ also. Since $\lambda = 1$, the difference $x$ can only occur once between elements of $D$. Since $x, 2x, 4x, 5x \in D$, this requires that $\{5x, 4x\} = \{2x, x\}$. If $x = 5x$, then 111 divides $4x$, which is impossible. If $x = 4x$, then 111 divides $3x$, which requires $x \in \{0, 37, 74\}$. Since this holds for all $x \in D$, only three values are allowed to occur in our difference set of size 10.

13.2.20. Forbidding projective planes. 

a) If $m = x^2 + y^2$, where $m$ is an integer and $x$ and $y$ are rational, then the odd primes with odd power in the prime factorization of $m$ are congruent to 1 modulo 4. Let $c$ be the least common multiple of the denominators of $x$ and $y$ as fractions in lowest terms. Thus $mc^2 = a^2 + b^2$, where $a, b, c$ are all integers. The primes with odd power in $m$ are the primes with odd power in $mc^2$. Letting $r = mc^2$, it thus suffices to prove the statement for $r, a, c$.

So, we may assume that $x$ and $y$ are integers. Let $p$ be a prime congruent to 3 modulo 4 that divides $m$. We will prove that $p$ divides both $x$ and $y$. This yields $p^2|m$. Dividing the equation by $p^2$ then yields an expression for $m/p^2$ as the sum of two squares, and the claim follows by induction on the sum of the exponents in the prime factorization.

It thus suffices to show that $p$ divides $x$. If not, then $x$ has a multiplicative inverse modulo $p$. Since $m \equiv 0 \pmod{p}$, multiplying $x^2 + y^2 = m$ by a natural number congruent to $x^{-2}$ yields $1+(x^{-1}y)^2 \equiv 0 \pmod{p}$. When $p \equiv 3 \pmod{4}$, the number $-1$ is not a square, so there is no solution to $1+z^2 \equiv 0 \pmod{p}$. We conclude that $p | x$, and thus also $p | (m^2 - x^2)$.

Comment: The sufficiency of the condition is the famous Two Squares Theorem of Fermat, proved in Section 10.1 by the Pigeonhole Principle.

b) If $n$ is congruent to 1 or 2 modulo 4 and there is a projective plane of order $n$, then every odd prime with odd power in the prime factorization of $n$ is congruent to 1 modulo 4. The lines in a projective plane of order $n$ form a symmetric $(n^2 + n + 1, n + 1, 1)$-design. By the Bruck–Chowla–Ryser Theorem, this requires a nonzero integer solution to $z^2 = nx^2 + (-1)^{n(n+1)/2}y^2$, since here $k - \lambda = n$. When $n$ is congruent to 1 or 2 modulo 4, $n(n+1)/2$ is odd, and the equation becomes $y^2 + z^2 = nx^2$. Dividing by $x^2$ converts this to $n = a^2 + b^2$ with $a$ and $b$ rational. By part (a), all odd primes appearing with odd power in the prime factorization of $n$ are congruent to 1 modulo 4.

Comment: This result prohibits projective planes of orders 6, 12, 14, 15, 21, 22, 24, 28, 30, etc., but it does not prohibit projective planes of orders 10, 18, 20, 26, etc.

13.2.21. Construction of a $(41, 5, 1)$-design.

a) The translates of a $(v, k, \lambda)$-difference family form a $(v, k, \lambda)$-design.

b) The translates modulo 41 of $\{0, 1, 4, 11, 29\}$ and $\{0, 5, 14, 20, 22\}$ for a $(41, 5, 1)$-design. For $i \in \mathbb{Z}_{41}$ let $A_i = \{i, i+1, i+4, i+11, i+29\}$ and $B_i = \{i, i+5, i+14, i+20, i+22\}$. We claim that these 82 blocks $A_i, B_i$ form a $(41, 5, 1)$-design.

Within $A_0$ the 10 pairs form 20 differences, and the same is true for $B_0$. Furthermore, all these differences are distinct, as follows:

$$A_i: \pm 1, 3, 4, 7, 10, 11, 12, 13, 16, 18$$

$$B_i: \pm 2, 5, 6, 8, 9, 14, 15, 17, 19, 20$$
It suffices to show that every pair \( \{u, v\} \) is contained in one block. Each of the 40 differences appears as a difference in \( A_0 \) or in \( B_0 \) but not both. Hence each pair arises in exactly one of the translates of \( A_0 \) or one of the translates of \( B_0 \).

### 13.3. FURTHER CONSTRUCTIONS

#### 13.3.1. A resolvable \((v, 2, 1)\)-design when \( v \) is even.\(^1\) We have \( v \) points, and we want blocks of size 2, with every two points occurring together in exactly one block. Hence the blocks are the edges of \( K_v \). A parallel class corresponds to the edges of a perfect matching. When \( v \) is even, the edge-chromatic number of \( K_v \) is \( v - 1 \); that is, \( K_v \) decomposes into perfect matchings, and they form the parallel classes of a resolvable design.

#### 13.3.2. \( K_0 \) decomposes into 4-cycles, cyclically. The graph \( C_4 \) is graceful; with the vertices labeled 0, 1, 5, 3 in order, the edge differences are 1, 4, 2, 3. With the vertices equally spaced around a circle, the difference classes are 1, 2, 3, 4. Hence the nine rotations of 4-cycle with vertices \( i, i + 1, i + 5, i + 3 \) in order cover all nine edges in each difference class.

#### 13.3.3. Caterpillars are graceful. Let \( G \) be a caterpillar with \( m \) edges. A longest path can be chosen as the spine, and each edge not along the spine has one endpoint on the spine.

**Proof 1** (induction on \( m \)). We prove the stronger statement that every caterpillar has a graceful number such that any specified endpoint of the spine is numbered 0 and another where it is numbered \( m \). This is immediate when \( m = 0 \) (or \( m = 1 \)).

For the induction step it suffices to produce a graceful numbering with 0 or \( m \) at an endpoint of the spine, since subtracting all labels from \( m \) yields a graceful numbering of the opposite type. Let \( v \) be an endpoint of the spine of \( G \), and let \( u \) be the neighbor of \( v \) in \( G \). If \( v \) is an endpoint of the spine of the caterpillar \( G - v \), then use the numbering of \( G - v \) that numbers \( u \) as 0 and give number \( m \) to \( v \). Otherwise, in \( G - v \) there is another leaf neighbor \( w \) of \( u \), ending a spine of the same length as \( G \). Using a graceful numbering of \( G - v \) that has label \( m - 1 \) at \( w \) (since \( G - v \) has \( m - 1 \) edges) will put label 0 at \( u \), and then we complete the desired numbering of \( G \) by using \( m \) on \( v \).

**Proof 2** (properties of caterpillars). A caterpillar is a bipartite graph. It can be drawn on a channel between two parallel lines, with the vertices of one part of the bipartition on one line and the vertices of the other part on the other line. The edges can then be added within the channel between the two parts without crossings. This numbers the edges in order from \( m \) to 1 as they are encountered along the channel.

Starting with 0 and \( m \) on the endpoints of edge \( m \), each successive edge introduces a new vertex on the high side or the low side. If on the high side, the new vertex gets the highest unused label. On the low side, it gets the lowest unused label. This new label differs by 1 from the vertex of the previous edge that is being replaced, so the difference on this new edge is smaller by 1 than on the previous edge. When all edges have been encountered, all numbers from 0 to \( m \) have been assigned, and the edge differences from \( m \) to 1 have been established.

#### 13.3.4. A \((5, 3, 1, 2)\)-mixed difference system. \(\{0_2, 1_2, 2_2\}, \{1_1, 4_1, 0_2\}, \{2_1, 3_1, 0_2\}, \{1_1, 4_1, 2_2\}, \{2_1, 3_1, 2_2\}, \{0_1, 0_2, 2_2\}\)

#### 13.3.5. the blocks described in ?? form a \((u, 3, 1, 3)\)-mixed difference system, thus yielding an STS(v) whenever \( v \equiv 3 \pmod{6} \).

#### 13.3.6. The complete k-partite graph \( G \) with parts of size \( k \) decomposes into \( k^2 \) copies of \( K_k \) if and only if there is an affine plane of order \( k \). Note first that \( G \) has \( \binom{k}{2} k^2 \) edges, which is the number of edges in \( k^2 \) edge-disjoint copies of \( K_k \).

First consider an affine plane of order \( k \). It is a resolvable \((k^2, k, 1)\)-design obtained from a projective plane by deleting the points in one line \( L \). The \( k \)-sets obtained from the \( k \) lines other than \( L \) that contained the same point on \( L \) form a parallel class; there are \( k + 1 \) such classes. Distinguish one class as partitioning the \( k^2 \) points into the \( k \) parts of \( G \). Each other line in the affine plane intersects each of these parts in one point and hence consists of the vertices of a copy of \( K_k \) in \( G \). Since no two lines in the plane share two points, the resulting copies of \( K_k \) are edge-disjoint. Since there is the right number of them, they decompose \( G \).

Conversely, consider such a decomposition of \( G \). It consists of \( k^2 \) copies of \( K_k \) on the \( k^2 \) vertices of \( G \). We claim that these sets, together with the \( k \) parts of \( G \) (which also have size \( k \)) form the blocks of a \((k^2, k, 1)\)-design. From the necessary conditions \( bk = vr \) and \( r(k - 1) = \lambda(v - 1) \), we have \( b = \frac{v}{k} k + 1 = k(k + 1) \), so this is the correct number of blocks. Each element appears in one special block and \( k(k - 1)/(k - 1) \) copies of \( K_k \), so they all appear in the same number of blocks. Finally, every two vertices of \( G \) appear together in exactly one block: it is a special block if they lie in the same part, and it is a copy of \( K_k \) otherwise, since in a decomposition of \( G \) each edge appears in exactly one of those copies. Hence this set of block satisfies all the required properties to form a \((k^2, k, 1)\)-design.

#### 13.3.7. Difference triples to cyclic STS.
13.3.8. A graphical $(6, 3, 2)$-design. A $(6, 3, 2)$-design has six points, with triples for blocks. Since $r = \lambda(v - 1)/(k - 1)$, each point must appear in five triples. Since $bk = vr$, there must be 10 blocks. Each pair of points should appear in two blocks.

Put five points on a circle and one point in the center. Create five Type 1 blocks that each consist of three consecutive vertices along the circle. Create five more Type 2 blocks that each consist of the central point and two non-consecutive points on the circle.

Two consecutive points on the circle appear together in two Type 1 blocks. Two non-consecutive points on the circle appear together in one Type 1 block and one Type 2 block. The central point and any point on the circle appear together in two Type 2 blocks.

13.3.9. There is no cyclic STS$(9)$. A Steiner triple system of order 9 is a $(9, 3, 1)$-design; it has 12 blocks. If the blocks lie in cyclically invariant classes, then the sizes of these classes must be 9 and 3 (or four classes of size 3). A cyclically invariant class of size 3 has a block that rotates into itself after three shifts. Labeling the elements cyclically, we may assume that the elements are $Z_9$ and that the class of size 3 is generated by $\{0, 3, 9\}$.

The blocks of this class contain precisely the pairs of elements whose difference is divisible by 3. The other class must cover the pairs with differences in the set $\{\pm1, \pm2, \pm4\}$. Since no three of these differences sum to 0 modulo 9, the other class cannot cover the remaining pairs.

13.3.10. Complete Theorem 13.3.33.

13.3.11. Stronger Fisher inequality.

13.3.12. Design from finite field.

13.3.13. Affine planes.

a) If $B$ is a block in a $(q^2, q, 1)$-design, and $x$ is an element not in $B$, then there is a unique block in the design that contains $x$ and is disjoint from $B$. Each element of $B$ must appear with $x$ in exactly one block. No two of these elements can appear in the same block containing $x$, since they already appear together in $B$. Hence exactly $q$ blocks containing $x$ intersect $B$. However, the total number of blocks containing $x$ (or any element) in any $(v, k, \lambda)$-design is $(v - 1)\lambda/(k - 1)$, which here equals $q + 1$. Hence exactly one block containing $x$ is disjoint from $B$.

b) Every $(q^2, q, 1)$-design is resolvable. For any block $B$ and $x$ not in $B$, let $B(x)$ be the block given by part (a). If $y \in B(x)$, then $B(y) = B(x)$, since already $B(x)$ is disjoint from $B$ and contains $y$. Thus the blocks disjoint from $B$ form a partition of the elements outside $B$. Together with $B$, they form a parallel class consisting of $q$ blocks of size $q$. Since this holds for every $B$, the blocks group into parallel classes, making the design resolvable.

c) If there is a $(q^2, q, 1)$-design, then there is a $(q^2 + 1, q, q - 1)$-design. The desired design puts each element in $q^2$ blocks, and the total number of blocks should be $q(q^2 + 1)$. The original design has $q(q + 1)$ blocks.

Repeat each block in the original design $q - 1$ times, except for those in one parallel class $C$. Include the blocks of $C$ once. Also introduce a new element $z$. Form $q^2$ blocks containing $z$ by substituting $z$ once for each of the $q$ elements in each of the $q$ blocks in $C$. Note that the number of blocks is $q^2(q - 1) + q + q^2$, the desired total.

Each pair of elements that did not appear in a block in $C$ now appears in $q - 1$ blocks. This also holds for pairs in a block $B$ in $C$; they appear together once in the copy of $C$ and in $q - 2$ of the substituted blocks where $z$ substitutes for one of the $q - 2$ elements of $B$ other than these two. Finally, $z$ appears with each of the $q^2$ other elements exactly $q - 1$ times, when substituting for another element of its block in $C$.

13.3.14. PBD to get $N(24) \geq 4$.

13.3.15. Pairwise-balanced designs.

a) A $(v, \{3, 5\}, 1)$-PBD exists only when $v$ is odd, and one exists for $v = 11$. The block sizes allowed are 3 and 5. An element appearing in $s$ blocks of size 3 and $t$ of size 5 appears with other elements in $2s + 4t$ pairs. This value is even and must equal $v - 1$, so $v$ must be odd.

For the construction, start with a resolvable $(6, 2, 1)$-design (a decomposition of $K_2$ into five perfect matchings), and follow Example 13.3.27. There are five parallel classes. Add one element for each parallel class, entering all the blocks of that class. Together with the old elements in blocks of size 3, the old elements still appear together once because we augmented all old blocks with new elements.

b) A $(v, \{4, 5\}, 1)$-PBD exists only when $v$ or $v - 1$ is divisible by 4, and one exists for $v = 17$. The block sizes allowed are 4 and 5. With $s$ blocks of size 4 and $t$ of size 5, the total number of pairs is $6s + 10t$. This value is even and must equal $v(v - 1)/2$, so $v$ or $v - 1$ must be divisible by 4.

For the construction, start with the affine plane of order 4, a resolvable $(16, 4, 1)$-design. Add one element $z$, and add $z$ to each block in one parallel class. The blocks in the remaining classes remain untouched at size 4 (so the statements in Example 13.3.27 about block sizes are not quite correct), while the new blocks containing $z$ have size 5. No extra block is needed for the added element(s).

13.3.16. More PBD
Chapter 13: Combinatorial Designs

13.3.17. Furedi $K_{2,t+1}$-free.

13.3.18. Explicit 10 by 10 pair.

13.3.19. PBD and matroid.

13.3.20. Permutations and latin squares.


a) If a graph $G$ with $m$ edges has a graceful labeling, then $K_{2m+1}$ decomposes into $2m+1$ copies of $G$. View the vertices of $K_{2m+1}$ as the congruence classes modulo $2m+1$, arranged cyclically. The difference between congruence classes $r$ and $s$ is the value in $\{1, \ldots, m\}$ congruent to $r-s$ or $s-r$. Group the edges of $K_{2m+1}$ by the difference between the endpoints. For $1 \leq j \leq m$, there are $2m+1$ edges with difference $j$.

A graceful labeling of $G$ yields copies of $G$ in $K_{2m+1}$ called $G_0, \ldots, G_{2m}$. The vertices of $G_i$ lie in $\{k, \ldots, k+m\}$ (modulo $2m+1$), with $k+i$ adjacent to $k+j$ if and only if $i$ is adjacent to $j$ in the graceful labeling of $G$. Thus $G_0$ is the original gracefully labeled $G$. Each difference class has one edge in each $G_k$, and $G_0, \ldots, G_{2m}$ is a decomposition of $K_{2m+1}$.

b) If the Graceful Tree Conjecture holds and $G$ is a tree with $m$ edges, then $K_{2m}$ decomposes into $2m-1$ copies of $G$. Let $G' = G - u$, where $u$ is a leaf of $G$ with neighbor $v$. Let $w$ be a vertex of $K_{2m}$. Construct a cyclic $G$-decomposition of $K_{2m} - w$ using a graceful labeling of $G'$ as in the proof of part (a). In this construction, each vertex serves as $v$ in exactly one copy of $G'$. Extend each copy of $G'$ to a copy of $G$ by adding the edge to $w$ from the vertex serving as $v$. This exhausts the edges to $w$ and completes the $G$-decomposition of $K_{2m}$.

13.3.22. If a bipartite graph $G$ with $m$ edges has an $\alpha$ labeling, and $K_{2nk+1}$ decomposes into $(2mk+1)k$ copies of $G$. An $\alpha$-labeling of a bipartite graph $G$ is a graceful labeling such that all labels of one part are smaller than all labels of the other part.

View $V(K_{2mk+1})$ as $Z_{2mk+1}$. Let $f$ be an $\alpha$-labeling of an $X, Y$-bigraph $G$, with $\text{max}_{x \in X} f(x) < \text{min}_{y \in Y} f(y)$. For $0 \leq i \leq k-1$, let $B_i$ be the copy of $G$ in which every $x \in X$ is viewed as vertex $f(x)$ and every $y \in Y$ is viewed as $f(y) + mi$. The translates of $B_0, \ldots, B_{k-1}$ modulo $2mk+1$ decompose $K_{2mk+1}$ into copies of $G$.

Let $S = \{f(x): x \in X\}$. Because the differences along edges of $G$ are 1 through $m$, the differences between vertices along edges of $B_i$ are $mi+1$ through $(m+1)i$. Hence $B_0, \ldots, B_{k-1}$ together capture one edge of each difference class in $Z_{2mk+1}$. Rotating this set of subgraphs then gives all of each difference class.

13.3.23. Graceful Eulerian graphs.

a) When $G$ is a graceful Eulerian graph with $m$ edges, $m$ or $m+1$ is divisible by 4. Let $f$ be a graceful labeling. The parity of the sum of the labels on an edge is the same as the parity of their difference. Hence the sum $\sum_{v \in V(G)} d(v)f(v)$ has the same parity as the sum of the edge differences. The first sum is even, since $G$ is Eulerian. The second has the same parity as the number of odd numbers in $[m]$. This is even if and only if $m$ or $m+1$ is divisible by 4.

b) The condition of part (a) is sufficient when $G$ is a cycle. We show that $C_n$ is graceful when 4 divides $n$ or $n+1$. We show an explicit construction ($n = 16$ and $n = 15$) and a general construction for each congruence class. In the class where $n+1$ is divisible by 4, we let $n'$ denote $n+1$. When $n$ is divisible by 4, let $n' = n$.

The labeling uses a base edge joining 0 and $n'/2$, plus two paths. The bottom path, starting from 0, alternates labels from the top and bottom to give the large differences: $n$, $n-1$, and so on down to $n'/2+1$. The top path, starting from $n'/2$, uses labels working from the center to give the small differences: 1, 2, and so on up to $n'/2-1$. The label next to $n'/2$ is $n'/2 - 1$ when 4 divides $n$, otherwise $n'/2 + 1$. When chosen this way, the two paths reach the same label at their other ends to complete the cycle: $n/4$ in the even case, $3n'/4$ in the odd case. Checking this ensures that the intervals of labels used do not overlap. Note that the value $3n/4$ is not used in the even case, and $n'/4$ is not used in the odd case.
13.3.24. The graph consisting of \( k \) copies of \( C_4 \) with one common vertex is graceful. The construction is illustrated below for \( k = 4 \). Let \( x \) be the central vertex. Let the neighbors of \( x \) be \( y_0, \ldots, y_{2k-1} \), and let the remaining vertices be \( z_0, \ldots, z_{k-1} \), such that \( N(z_i) = \{y_{2i}, y_{2i+1}\} \).

Define a labeling \( f \) by \( f(x) = 0 \), \( f(y_i) = 4k - 2i \), and \( f(z_i) = 4i + 1 \). The labels on \( y_1, \ldots, y_{2k} \) are distinct positive even numbers, and those on \( z_1, \ldots, z_k \) are distinct odd numbers, so \( f \) is injective, as desired. The differences on the edges from \( x \) are the desired distinct even numbers.

The differences on the remaining edges are odd and less than \( 2k \); it suffices to show that their values are distinct. Involving \( z_i \), the differences are \( 4k - 1 - 8i \) and \( 4k - 3 - 8i \). Starting from \( z_0 \) through increasing \( i \), these are \( 4k - 1, 4k - 3, 4k - 9, 4k - 11, \ldots \). Starting from \( z_{k-1} \) through decreasing \( i \), these are \( -4k + 5, -4k + 7, -4k + 13, -4k + 15, \ldots \). The absolute values are distinct, as needed.

13.3.25. No OP(3,3), construct OP(3,4).
13.3.27. Resolvability of \((15,3,1)\)-design.
13.3.28. \((21,5,3)\)-design for \( t = 3 \).
13.3.29. Transversal design.