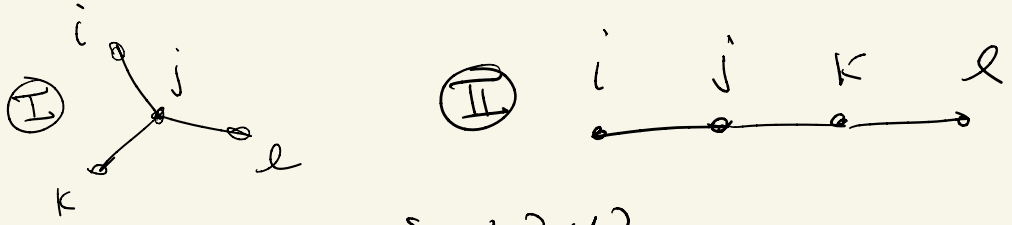
PRACTICE Exam MAT2250
Suggested solutions

Problem 1

1. The spanning trees of K_4 are of two types



where $\{i,j,k,\ell\} = \{1,2,3,4\}$

Type (I) is determined by choice of $j \in \{1,2,3,4\} \Rightarrow$ There are $\underline{4}$ such spanning trees

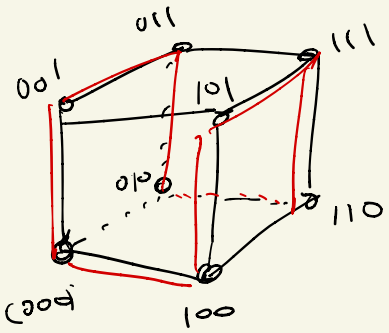
Type (II) is determined by an ordering of $\{1,2,3,4\}$ and the reverse ordering $\Rightarrow$ There are $\frac{4!}{2} = \underline{12}$ types

# of spanning trees of K_4 is $\underline{16}$.

2. The vertices of the hypercube graph Q_n are in bijection with binary words of length n. Hence there are 2^n vertices in Q_n

3. A graph is Eulerian if and only if every vertex is of even degree. For the graph Q_n $\deg(v) = n$ for any $v \in Vert(Q_n)$. Hence Q_n is Eulerian if and only if n is even

4. A Hamiltonian circuit in G is a circuit which visits every vertex exactly once.



A Hamiltonian circuit in Q_3 is the sequence of vertices:

$000 - 100 - 101 - 111 - 110 - 010 - 011 - 001 - 000$

Problem 2.

1) For $n = p^k$ for p prime $k \in \mathbb{N}$ there are $p^k - 1$ mutually orthogonal latin squares of order n.

since $9 = 3^2$ there are 8 mutually orthogonal latin squares of order 9.

2) A 2-design with parametes $\lambda = 1$, $k = 3$, $v = 7$ is a pair $(S, \mathcal{B})$ where S is a finite set with $|S| = 7$ and $\mathcal{B} = \{B_1, \dots, B_4\}$ is a collection of subsets of S

such that:

- $|B_i| = k$ for all $B_i \in \mathcal{B}$.
- every $I \subseteq S$ with $|I| = 2$ is contained in exactly $\lambda = 1$ of the B_i's.

To find how many elements of $\mathcal{B}$ contain a fixed element $i \in S$.

$$A_i = \{(j, B) \text{ s.t. } \{i, j\} \subset B_i\}.$$

Then $|A_i| = 6 \cdot \lambda = 6$. and also $|A_i| = \#\text{blocks containing } i \cdot (k-1)$.

$$\Rightarrow \frac{6}{(k-1)} = \#\text{blocks containing } i \Rightarrow$$

each i is contained in $\underline{3}$ blocks

3. The $(ik)^{th}$ entry of $B \cdot B^T$ is the inner product of the zero one vectors:

$$(b_{ij_1} \dots b_{ij_b}) \cdot (b_{kj_1} \dots b_{kj_b})$$

Since $\{i k\}$ are contained in a unique block if $i \neq k$ there exists a unique j_s s.t. $b_{ij_s} = b_{kj_s} = 1$ otherwise one is zero and the other is 1.

$(b_{ij_1} \dots b_{ij_b}) \cdot (b_{ij_1} \dots b_{ij_b})$ is equal to the # of blocks containing i. Which is equal to.

$$r = \frac{bk}{v}.$$

Problem 3

1. Let A be a finite set. The Hamming distance on A^n is $\Delta(a,b) := |\{ i \mid a_i \neq b_i \}|$ for $a = (a_1 \cdots a_n)$, $b = (b_1 \cdots b_n) \in A^n$.

Claim Δ satisfies the triangle inequality. That is $\Delta(a,b) \leq \Delta(a,c) + \Delta(c,b)$ $\forall$ $a,b,c \in A^n$.

$$\Delta(a,b) := |\{ i \mid a_i \neq b_i \}|$$
$$= |\{ i \mid a_i \neq b_i, a_i = c_i, b_i \neq c_i \}|$$
$$+ |\{ i \mid a_i \neq b_i, a_i \neq c_i \ b_i = c_i \}|$$
$$+ |\{ i \mid a_i \neq b_i, a_i \neq c_i \ b_i \neq c_i \}|.$$

$\leq |\{i \mid a_i \neq c_i\}| + |\{i \mid c_i \neq b_i\}|.$

$\Delta(a,c) + \Delta(c,b).$

Hence Δ satisfies the triangle inequality.

2. $\Delta(00000, c) = w(c)$ and

$\min_{c \neq 0,\ c \in C} w(c) = 2.$

$\Delta(21212, 01010) = 3$

$\Delta(21212, 20202) = 2$

$\Delta(01010, 20202) = 5$

Hence $d(C) = 2.$

3 Recall the correspondence of code words and polynomials

$$C = (c_{n-1}, \ldots c_1, c_0) \mapsto c(x) = \sum_{i=0}^{n-1} c_i x^i$$

under this correspondence

$$C_i = \{ c \mid g_i(x) \mid c(x) \}.$$

Claim $C_1 \subseteq C_2$ if and only if

$$g_2(x) \mid g_1(x).$$

if $c \in C_1 \Rightarrow g_1(x) \mid c(x)$. since $g_2(x) \mid g_1(x)$ then $g_2(x) \mid c(x)$ hence $c \in C_2$ □.

Now we verify that $g_2(x) \mid g_1(x)$

Notice that $(x+1) g_2(x) = g_1(x)$ since

$$(x+1)(x^3+x^2+1) = x^4+x^3+x+x^3+x^2+1$$
$$= x^4+x^2+x+1$$

Problem 4

1) $3^7 = 3^{1+2+4} = 3 \cdot 3^2 \cdot 3^4$

$\equiv 3 \cdot 9 \cdot 3^3 \cdot 3 \equiv 27 \cdot 27 \cdot 3 \equiv 3 \bmod 13$

2) The multiplicative inverse of 2 mod 11 can be checked

$2 \cdot 2 = 4 \not\equiv 1 \bmod 11$

$2 \cdot 3 \equiv 6 \not\equiv 1 \bmod 11$

$2 \cdot 4 = 8 \not\equiv 1$

$2 \cdot 5 = 10 \equiv -1$

$2 \cdot 6 = 12 \equiv 1 \bmod 11.$

The element 6 does not have a multiplicative inverse mod 15 since $6 \cdot 5 \equiv 0 \mod 15$.

3. We start by computing the powers of 7 mod 11.

$7^1 \equiv 7$

$7^2 \equiv 5$

$7^3 \equiv 5 \cdot 7 \equiv 2$

$7^4 \equiv 7 \cdot 2 \equiv 3$

$7^5 \equiv 7 \cdot 3 \equiv 10$

$7^6 \equiv 7 \cdot 10 \equiv 4$

$7^7 \equiv 7 \cdot 4 \equiv 6$

$7^8 \equiv 6 \cdot 7 \equiv 9$

$7^9 \equiv 9 \cdot 7 \equiv 8$

$7^{10} \equiv 8 \cdot 7 \equiv 1$.

If Alice sends $A = 2$ to Bob then Alice's private key is $a = 3$ since $7^3 \equiv 2 = A \mod 11$

Similarly Bob's private key is $b = 5$ since $7^5 \equiv 10 = B \mod 11$.