SOLUTIONS TO SOME OF THE PROBLEMS IN MAT3250 SPRING 2025

ANNE BRUGÅRD

Week 3 – Recurrence relations and generating functions

Warm up.

(1) $x^{\overline{3}} = x(x+1)(x+2) = x^3 + 3x^2 + 2x$. Let $N = \{1, 2, 3\}$ We have

$$\begin{aligned} s_{3,3} &= 1 \qquad (1)(2)(3) \\ s_{3,2} &= 3 \qquad (12)(3), (13)(2), (23)(1) \\ s_{3,1} &= 2 \qquad (123), (132) \end{aligned}$$

We see that $s_{3,i} = a_i$, where a_i is the coefficient of x^i.

$x^{\overline{4}} = x(x+1)(x+2)(x+3) = x^4 + 6x^3 + 11x^2 + 6x$. We have

$$\begin{aligned} s_{4,4} &= 1 \\ s_{4,3} &= 6 \\ s_{4,2} &= 11 \\ s_{4,1} &= 6 \end{aligned}$$

(2) We use that $\frac{x^{\underline{k}}}{k!} = \binom{x}{k}$ and the recurrence relation $\binom{x}{k} = \binom{x-1}{n} + \binom{x-1}{n-1}$.

$$\frac{x^{\underline{k}}}{k!} = \frac{(x-1)^{\underline{k}}}{k!} + \frac{(x-1)^{\underline{k}}}{(k-1)!}$$

Multiplying each side by $k!$ give us the recurrence relation

$$x^{\underline{k}} = (x-1)^{\underline{k}} + k(x-1)^{\underline{(k-1)}}.$$

(3) Let $S(z)$ be the generating function of the sequence.
a)

$$\begin{aligned} S(z) &= \sum_{n=0}^{\infty} (a_n + 10b_n - c_n) z^n \\ &= \sum_{n=0}^{\infty} a_n z^n + 10 \sum_{n=0}^{\infty} b_n z^n - \sum_{n=0}^{\infty} c_n z^n \\ &= A(z) + 10B(z) - C(z) \end{aligned}$$

b)

$$\begin{aligned} S(z) &= \sum_{n=0}^{\infty} 2^n a_n z^n \\ &= \sum_{n=0}^{\infty} a_n (2z)^n \\ &= A(2z) \end{aligned}$$

c)

$$\begin{aligned} S(z) &= \sum_{n=0}^{\infty} (a_n + b_{n-1}) z^n \\ &= \sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} b_{n-1} z^n \\ &= A(z) + z \sum_{n=0}^{\infty} b_n z^n \\ &= A(z) + zB(z) \end{aligned}$$

d)

$$\begin{aligned} S(z) &= \sum_{n=0}^{\infty} (a_n + 1) z^n \\ &= \sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} z^n \\ &= A(z) + \frac{1}{1-z} \end{aligned}$$

e)

$$\begin{aligned} S(z) &= \sum_{n=0}^{\infty} (n a_n) z^n \\ &= z \sum_{n=0}^{\infty} n a_n z^{n-1} \\ &= z A'(z) \end{aligned}$$

(4) a)

$$\begin{aligned} \frac{x}{1-2x} &= x \frac{1}{1-2x} \\ &= x \sum_{n=0}^{\infty} (2x)^n \\ &= \sum_{n=0}^{\infty} 2^n x^{n+1} \end{aligned}$$

b)

$$\frac{1}{(1-x)^2} = (\frac{1}{(1-x)})' = (\sum_{n=0}^{\infty} x^n)' = \sum_{n=0}^{\infty} nx^{n-1} = \sum_{n=0}^{\infty}(n+1)x^n$$

c)

$$\begin{aligned}\frac{1}{1-x-y} &= \frac{1}{1-(x+y)} \\ &= \sum_{n=0}^{\infty}(x+y)^n \\ &= \sum_{n=0}^{\infty}\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}\end{aligned}$$

Problem 3.1. Prove the following recurrence formula for Stirling numbers of the second kind:

$$S_{n+1,k+1} = \sum_{i=k}^{n}\binom{n}{i}S_{i,k}.$$

Hint: Empathize with the element $n+1$ and partition the set of all $(k+1)$-set partitions of $\{1,\dots n+1\}$ based on the size o the subset in the partition containing $n+1$.

Solution. We follow the hint and partition the set of all $(k+1)$-set partitions based on the size of the subset in the partition that contains the element $(n+1)$. Since we have $(k+1)$ subsets in total, the size of the subset that contains the element $n+1$ can be at most $n-k+1$. In that case, we have k subsets each containing one element and the $n-k+1$-subset containing $n-k$ elements and the element $n+1$. We can make this partition in

$$\binom{n}{k}S_{k,k}$$

ways, where $\binom{n}{k}$ counts the number of ways we can choose the elements not in the subset containing the element $n+1$ and $S_{k,k}$ counts the numbers of ways to partition k elements into k subsets (which is one way).

The next possible size of the subset that contains the element $n+1$ is $n-k$. In that case $k+1$ elements are not in this subset and we have to count the number of ways to choose these $k+1$ elements and the number of ways to partition these $k+1$ elements into k subsets. The number is

$$\binom{n}{k+1}S_{k+1,k}.$$

Following this procedure when we let the subset that contains the element $n+1$ be smaller and smaller, we get the formula

$$S_{n+1,k+1} = \sum_{i=k}^{n}\binom{n}{i}S_{i,k}.$$

Problem 3.2. Let $P_{n,k}$ be the number of integer partitions of n with k parts.

(1) Give a combinatorial proof of the following relation for integer partitions:

$$P_{n,k} = \sum_{n=0}^{k} P_{n-k,i}$$

What initial conditions need to be fixed in order to make this a recurrence relation giving all numbers of $P_{n,k}$? *Hint: Remove the first column from the Young diagram of a partition of n with k parts and count what remains.*

Solution.

(1) We follow the hint and remove the first column from the Young diagram of a partition of n with k parts and count what remains. When we have removed the first column, what remains is a partition of $n-k$ elements. The number of parts in the partition of $n-k$ elements can be between 1 and k depending on the partition of n elements into k parts was before we removed the first column. If none of the numbers in the partition was 1, then we have a partition of $n-k$ elements into k parts (try drawing the Young diagram of the partition $7 = 3+2+2$ and remove the first column). If every number in the partition is 1 expect for one (the number $n-k+1$), then we have a partition of $n-k$ elements into k parts after removing the first column (try doing this for $7 = 5+1+1$).

In general after removing the first column, we get a partition of $n-k$ elements into i parts when the partition of n elements into k parts has $k-i$ ones. We therefore sum over $P_{n-k,i}$ for $i = 0$ to n and get the formula

$$P_{n,k} = \sum_{n=0}^{k} P_{n-k,i}$$

Problem 3.3. Let an be the number of ways a $2 \times n$ rectangle can be covered by 1×2 dominoes. Give a recurrence relation for the sequence (a_n). What does this tell you about $A(z) = \sum_{n=0}^{\infty} a_n z^n$?

Let b_n be the number of ways a $3 \times n$ rectangle can be covered by 1×3 dominoes. Determine a recurrence relation for (b_n) and explain what this means for$B(z) = \sum_{n=0}^{\infty} b_n z^n$.

Solution. $a_n = a_{n-1} + a_{n-2}$ valid for $n \geq 2$. For the relation to be right for $a_2 = 2$, we must have $a_0 = a_1 = 1$. This gives

$$\begin{aligned} F(z) &= \sum_{n=0}^{\infty} a_n z^n \\ &= 1 + z + \sum_{n=2}^{\infty} a_{n-1} z^n + \sum_{n=2}^{\infty} a_{n-2} z^n \\ &= 1 + z + z \sum_{n=1}^{\infty} a_n z^n + z^2 \sum_{n=0}^{\infty} a_n z^n \end{aligned}$$

$$\begin{aligned}
&= 1 + z + z(-1 + \sum_{n=0}^{\infty} a_n z^n) + z^2 \sum_{n=0}^{\infty} a_n z^n \\
&= 1 + zF(z) + z^2 F(z) \\
F(z) &= \frac{1}{1 - z - z^2}.
\end{aligned}$$

$b_n = b_{n-3} + b_{n-1}$ valid for $n \geq 3$. For the relation to be right for $b_3 = 2$, we must have $b_0 = b_1 = b_2 = 1$

$$\begin{aligned}
F(z) &= \sum_{n=0}^{\infty} b_n z^n \\
&= 1 + z + z^2 + \sum_{n=3}^{\infty} b_{n-1} z^n + \sum_{n=3}^{\infty} b_{n-3} z^n \\
&= 1 + z + z^2 + z \sum_{n=2}^{\infty} b_n z^n + z^3 \sum_{n=0}^{\infty} b_n z^n \\
&= 1 + z + z^2 + z(-1 - z + \sum_{n=0}^{\infty} b_n z^n) + z^3 \sum_{n=0}^{\infty} b_n z^n \\
&= 1 + zF(z) + z^3 F(z)
\end{aligned}$$

Solving this for $F(z)$ gives

$$F(z) = \frac{1}{1 - z - z^3}.$$

Week of 10 Feb - Generating functions continued

Warm-ups.

(1) Let the sequence a_n be defined by the recurrence $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ and $a_0 = 1$, $a_1 = 1$, $a_2 = 1$. Find an expression of the generating function for a_n as a rational function (do not find the partial fraction decomposition).

(2) Suppose the generating function of a sequence a_n is given by

$$A(z) = \frac{1}{(1-z)^2} + \frac{2}{1-2z}.$$

Give a formula for a_n as in Theorem 3.1. of Aigner.

(3) Find the closed form for the exponential generating function for the sequence given by the number of permutations of a set of size n.

Solution.

(1)

$$\begin{aligned} A(z) = \sum_{n=0}^{\infty} a_n z^n &= 1 + z + z^2 + \sum_{n=3}^{\infty} a_n z^n \\ &= 1 + z + z^2 + \sum_{n=3}^{\infty} (a_{n-1} + a_{n-2} + a_{n-3}) z^n \\ &= 1 + z + z^2 + z \sum_{n=2}^{\infty} a_n z^n + z^2 \sum_{n=1}^{\infty} a_n z^n + z^3 \sum_{n=0}^{\infty} a_n z^n \\ &= 1 + z + z^2 + z(A(z) - 1 - z) + z^2(A(z) - 1) + z^3 A(z) \\ &= 1 + z + z^2 - z - z^2 - z^2 + A(z)(z + z^2 + z^3) \\ &= 1 - z^2 + A(z)(z + z^2 + z^3). \end{aligned}$$

This gives

$$A(z) = \frac{1 - z^2}{1 - z - z^2 - z^3}.$$

(2)

$$\begin{aligned} A(z) &= \frac{1}{(1-z)^2} + \frac{2}{1-2z} \\ &= \sum_{n=0}^{\infty} (n+1) z^n + 2 \sum_{n=0}^{\infty} (2z)^n \\ &= \sum_{n=0}^{\infty} (n + 1 + 2^{n+1}) z^n. \end{aligned}$$

(3) The number of permutations of a set of size n is $n!$, so $a_n = n!$.

$$\begin{aligned} \hat{A}(z) &= \sum_{n=0}^{\infty} \frac{a_n}{n!} z^n \\ &= \sum_{n=0}^{\infty} \frac{n!}{n!} z^n \end{aligned}$$

$$\begin{aligned} &= \sum_{n=0}^{\infty} z^n \\ &= \frac{1}{1-z} \end{aligned}$$

Problem 4.1. Give the partial fraction decomposition of

$$\frac{1}{1-3z+2z^2}$$

and use this to compute the a_n given by

$$\frac{1}{1-3z+2z^2} = \sum_{n=0}^{\infty} a_n z^n.$$

What is the recurrence relation satisfied by the sequence (a_n)? For which n is this relation valid?

Solution. Since $(1-3z+2z^2) = (1-2z)(1-z)$, we have

$$\begin{aligned} \frac{1}{1-3z+2z^2} &= \frac{a}{1-2z} + \frac{b}{1-z} \\ 1 &= a(1-z) + b(1-2z) \\ 1 &= a+b-z(a+2b) \end{aligned}$$

So,

$$\begin{aligned} a+b &= 1 \\ a+2b &= 0, \end{aligned}$$

and $a = 2$, $b = -1$. We therefore get

$$\frac{1}{1-3z+2z^2} = \frac{2}{1-2z} - \frac{1}{1-z}.$$

We have

$$\begin{aligned} \frac{1}{1-3z+2z^2} &= \frac{2}{1-2z} - \frac{1}{1-z} \\ &= 2\sum_{n=0}^{\infty} (2z)^n - \sum_{n=0}^{\infty} z^n \\ &= \sum_{n=0}^{\infty} (2^{n+1}-1) z^n, \end{aligned}$$

so $a_n = 2^{n+1} - 1$.

Set $A(z) = \frac{1}{1-3z+2z^2} = \sum_{n=0}^{\infty} a_n z^n$. Then

$$\begin{aligned}
A(z) &= 1 + 3zA(z) - 2z^2A(z) \\
&= 1 + 3z\sum_{n=0}^{\infty} a_n z^n - 2z^2 \sum_{n=0}^{\infty} a_n z^n \\
&= 1 + 3\sum_{n=1}^{\infty} a_{n-1} z^n - 2\sum_{n=2}^{\infty} a_{n-2} z^n \\
&= 1 + 3(a_0 z^1 + \sum_{n=2}^{\infty} a_{n-1} z^n) - 2\sum_{n=2}^{\infty} a_{n-2} z^n \\
&= 1 + 3z + 3\sum_{n=2}^{\infty} a_{n-1} z^n - 2\sum_{n=2}^{\infty} a_{n-2} z^n \\
&= 1 + 3z + \sum_{n=2}^{\infty} (3a_{n-1} - 2a_{n-2}) z^n
\end{aligned}$$

This shows that $a_n = 3a_{n-1} - 2a_{n-2}$ for $n \geq 2$ and $a_0 = 1$, $a_1 = 3$.

Problem 4.2. Determine the recurrence relations, generating functions, and an explicit formula for the following sequences in n:

(1) The number of words of length n on an alphabet of size 5.
(2) The number of binary words of length n with no consecutive ones.
(3) The number of binary words of length n with an even number of zeros. *Let e_n and o_n be the number of words of length n with even and odd number of zeros, respectively. Give two relations between their generating functions $E(z)$ and $O(z)$.*

Solution.

(1) $a_n = 5^n$ for $n \geq 1$. $a_{n+1} = 5^{n+1} = 5 \cdot 5^n = 5a_n$, $a_1 = 5$.

$$A(z) = \sum_{n=0}^{\infty} 5^n z^n = \sum_{n=0}^{\infty} (5z)^n = \frac{1}{1-5z}.$$

(2) Let b_n be the number of words of length n with no consecutive ones. Such a word can end in either a 0 or a 1. If it end in a 0, the first $n-1$ letters can by any binary word of length $n-1$ with no consecutive ones. There are b_{n-1} such words. If it ends in 1, the $(n-1)$th letter must be a zero and the first $n-2$ letters can be any word of length $n-2$ with no consecutive ones. There are b_{n-2} such words. We therefore have $b_n = b_{n-1} + b_{n-2}$ for $n \geq 2$. We have $b_0 = 1$ and $b_1 = 2$. We find the generating function:

$$\begin{aligned}
B(x) &= 1 + 2x + \sum_{n=2}^{\infty} (b_{n-1} + b_{n-2}) \\
&= 1 + 2x + x\sum_{n=1}^{\infty} b_n x^n + x^2 \sum_{n=0} b_{n-2} x^n \\
&= 1 + 2x + x(-1 + \sum_{n=0}^{\infty} b_n x^n) + x^2 \sum_{n=0} b_{n-2} x^n \\
&= 1 + 2x - x + xB(x) + x^2 B(x)
\end{aligned}$$

$$B(x)(1-x-x^2) = 1+x$$
$$B(x) = \frac{1+x}{1-x-x^2}$$

We see that $b_n = F_{n+1}$, where (F_n) is the Fibonacci sequence with $F_0 = 0$ and $F_1 = 1$. We have from the Aigner that

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right),$$

so

$$b_n = F_{n+1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$

(3) Consider a binary word of length n with an even number of zeros. If the last word is 0, the first $n-1$ is a word with an odd number of zeros and if it ends in 1 the first $n-1$ is a word with an even number of zeros. We have $e_n = e_{n-1} + o_{n-1}$. In the same way we get $o_n = e_{n-1} + o_{n-1}$. We have $e_0 = 1$ and $o_0 = 0$, since the empty word has zero zeros which is even. Let $E(z) = \sum_{n=0}^{\infty} e_n z^n$ and $O(z) = \sum_{n=0}^{\infty} o_n z^n$. We have

$$\begin{aligned} E(z) &= 1 + \sum_{n=1}^{\infty}(e_{n-1} + o_{n-1})z^n \\ &= 1 + z\sum_{n=0}^{\infty}(e_n + o_n)z^n \\ &= 1 + zE(z) + zO(z). \end{aligned}$$

In the same way we get

$$O(z) = zE(z) + O(z).$$

We can now solve for $E(z)$. From the second equation we get

$$O(z) = \frac{zE(z)}{1-z}.$$

Substituting this into the first equation gives

$$\begin{aligned} E(z) &= 1 + zE(z) + \frac{z^2E(z)}{1-z} \\ E(z)(1 - z - z(1-z) - z^2) &= 1 - z \\ E(z)(1 - 2z + z^2 - z^2) &= 1 - z \\ E(z) &= \frac{1-z}{1-2z}. \end{aligned}$$

We use the generating function to find the recurrence relation.

$$\begin{aligned} E(z)(1-2z) &= 1-z \\ E(z) &= 1-z+2z\sum_{n=0}^{\infty} e_n z^n \\ &= 1-z+\sum_{n=1}^{\infty} 2e_{n-1}z^n \\ &= 1-z+2e_0 z+\sum_{n=2}^{\infty} 2e_{n-1}z^n, \end{aligned}$$

so $e_0 = 1, e_1 = -1+2e_0 = 1$ and $e_n = 2e_{n-1}$ for $n \geq 2$. We have $e_n = 2^{n-1}$ for $n \geq 1$.

Problem 4.3. From Problem 2.3, we know that $S_{n,2} = 2^{n-1} - 1$ for $n \geq 1$.

(1) Use this to express the generating function

$$S_2(z) = \sum_{n=0}^{\infty} S_{n,2} z^n$$

as a rational function.

(2) Use the recurrence relation $S_{n,k} = S_{n-1,k-1} + kS_{n-1,k}$ and the formula found for $S_2(z)$ to show

$$S_3(z) = \frac{z^3}{(1-z)(1-2z)(1-3z)}$$

(3) Use a partial fraction decomposition to find a closed formula for $S_{n,3}$.

Solution.

(1)

$$\begin{aligned} S_2(z) = \sum_{n=0}^{\infty} S_{n,2} z^n &= \sum_{n=1}^{\infty} (2^{n-1}-1)z^n \\ &= \sum_{n=1}^{\infty} 2^{n-1}z^n - \sum_{n=1}^{\infty} z^n \\ &= 1 + z\sum_{n=0}^{\infty} 2^n z^n - \sum_{n=0}^{\infty} z^n \\ &= 1 + z\sum_{n=0}^{\infty} (2z)^n - \sum_{n=0}^{\infty} z^n \\ &= 1 + \frac{z}{1-2z} - \frac{1}{1-z} \\ &= \frac{(1-2z)(1-z) + z(1-z) - (1-2z)}{(1-2z)(1-z)} \\ &= \frac{1-3z+2z^2+z-z^2-1+2z}{(1-2z)(1-z)} \\ &= \frac{z^2}{(1-2z)(1-z)} \end{aligned}$$

(2)

$$\begin{aligned}
S_3(z) &= \sum_{n=0}^{\infty} S_{n,3} z^n \\
&= \sum_{n=0}^{\infty} (S_{n-1,2} + 3S_{n-1,3}) z^n \\
&= \sum_{n=0}^{\infty} S_{n-1,2} z^n + 3 \sum_{n=0}^{\infty} S_{n-1,3} z^n \\
&= z \sum_{n=0}^{\infty} S_{n,2} z^n + 3z \sum_{n=0}^{\infty} S_{n,3} z^n \\
&= z \frac{z^2}{(1-2z)(1-z)} + 3z S_3(z) \\
&= \frac{z^3}{(1-3z)(1-2z)(1-z)}
\end{aligned}$$

(3)

$$\begin{aligned}
\frac{1}{(1-3z)(1-2z)(1-z)} &= \frac{a}{1-3z} + \frac{b}{1-2z} + \frac{c}{1-z} \\
1 &= a(1-2z)(1-z) + b(1-3z)(1-z) + c(1-3z)(1-2z) \\
&= a(1-3z+2z^2) + b(1-4z+3z^2) + c(1-5z+6z^2) \\
&= a+b+c-(3a+4b+5c)z + (2a+3b+6c)z^2.
\end{aligned}$$

This gives

$$\begin{aligned}
a+b+c &= 1, \\
3a+4b+5c &= 0, \\
2a+3b+6c &= 0.
\end{aligned}$$

Which has solutions $a = \frac{9}{2}$, $b = -4$, $c = \frac{1}{2}$, so we get

$$\begin{aligned}
S_3(z) &= \frac{9}{2(1-3z)} - \frac{4}{1-2z} + \frac{1}{2(1-z)} \\
&= \frac{9}{2} \sum_{n=0}^{\infty} (3z)^n - 4 \sum_{n=0}^{\infty} (2z)^n + \sum_{n=0}^{\infty} z^n \\
&= \sum_{n=0}^{\infty} \frac{1}{2}(3^{n+2} - 2^{n+3} + 1) z^n
\end{aligned}$$

This shows that $S_{n,3} = \frac{1}{2}(3^{n+2} - 2^{n+3} + 1)$.

Problem 4.4. Let F_n be the n-th Fibonacci number. Prove that

$$F_n = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-1-k}{k}.$$

Hint: Expand the generating function $F(z)$ as a sum over terms $z(z+z^2)^k$.

Solution.

$$\begin{aligned} F(z) = \sum_{n=0}^{\infty} F_n z^n = \frac{z}{1-z-z^2} &= \frac{z}{1-(z+z^2)} \\ &= z\sum_{l=0}^{\infty}(z+z^2)^l \\ &= z\sum_{l=0}^{\infty}\sum_{k=0}^{l}\binom{l}{k}z^k z^{2(l-k)} \\ &= \sum_{l=0}^{\infty}\sum_{k=0}^{l}\binom{l}{k}z^{2l-k+1} \end{aligned}$$

.

We fix an n and find the coefficient F_n in front of z^n. The coefficient is

$$F_n = \sum_{\substack{l=0,k=0 \\ 2l-k+1=n}} \binom{l}{k}$$

We rewrite the relation and get $k = 2l - n + 1$. This gives

$$F_n = \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor}\binom{l}{2l-n+1} = \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor}\binom{l}{n-1-l} = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor}\binom{n-1-i}{i},$$

where the first equality follows since $2l - n + 1 + (n - 1 - l) = l$. In the second equality we set $i = n - 1 - l$. $l = n - 1 - k$.

Problem 4.5. Let C_n be the Catalan numbers from Problem 2.6, and let $C(z)$ be their generating function.

(1) Prove that $C(z) = zC(z)^2 + 1$.
(2) Solve the quadratic equation to determine $C(z)$.
(3) Show that

$$C_n = 2 \cdot (-4)^n \binom{\frac{1}{2}}{n+1}.$$

Solution.

(1)

$$\begin{aligned} C(z) &= \sum_{n=0}^{\infty} C_n z^n \\ &= 1 + \sum_{n=1}^{\infty}\sum_{i=0}^{n-1}(C_i C_{n-1-i})z^n \\ &= 1 + z\sum_{n=0}^{\infty}\sum_{i=0}^{n}(C_i C_{n-i})z^n \\ &= 1 + z\sum_{n=0}^{\infty} C_n \cdot \sum_{n=0}^{\infty} C_n \end{aligned}$$

$$= 1 + zC(z)^2$$

(2) We use the *abc*-formula with $a = z$, $b = -1$,$c = 1$ and get

$$C(z) = \frac{1 \pm \sqrt{1-4z}}{2z}.$$

We have to decide which of the two solutions we want. We have that $C_0 = 1$, so $C(0) = \sum_{n=0}^{\infty} C_n z^n = C_0 0^0 + \sum_{n=1}^{\infty} C_n z^n = 1$. We consider the limits

$$\lim_{z\to 0^+} \frac{1+\sqrt{1-4z}}{2z} = \infty$$
$$\lim_{z\to 0^+} \frac{1-\sqrt{1-4z}}{2z} = \frac{\frac{4}{\sqrt{1-4z}}}{2\cdot 2} = 1,$$

where we used L'Hôpital's rule for the second limit. This shows that we want the negative sign.

(3)

$$\begin{aligned} C(z) = \frac{1-\sqrt{1-4z}}{2z} &= \frac{1-\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n}(-4z)^n}{2z} \\ &= \frac{1+(-1)-\sum_{n=1}^{\infty}\binom{\frac{1}{2}}{n}(-4z)^n}{2z} \\ &= -(2z)^{-1}\sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n+1}(-4z)^{n+1} \\ &= \sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n+1}(-2)^{-1}\cdot(-4)^{n+1}z^n \\ &= \sum_{n=0}^{\infty}\binom{\frac{1}{2}}{n+1}2\cdot(-4)^n z^n \end{aligned}$$

This shows that $C_n = 2\cdot(-4)^n\binom{\frac{1}{2}}{n+1}$.

Problem 4.6.

(1) Consider the product

$$F(x,y,z) = (x+y+z)^n = \sum_{i,j,k} a_{i,j,k} x^i y^j z^k$$

Explain why $a_{i,j,k}$ is the number of words on the alphabet $\{0,1,2\}$ of length n with i 0s, j 1s and k 2s.

(2) Let b_n be the number of words of length n on the alphabet $\{0,1,2\}$ with an even number of 0s and an even number of 1s. Show that

$$b_n = \frac{F(1,1,1)+F(-1,1,1)+F(1,-1,1)+F(-1,-1,1)}{4}$$

(3) Write the generating function of b_n as a rational function, and give a recurrence relating for the b_n.

Solution.

(1) The expansion of $(x+y+z)^n$ represent all the possible ways to choose n elements from the set $\{x,y,z\}$ where repetition is allowed. The coefficient $a_{i,j,k}$ represent the number of ways to choose i xs, j ys and k zs. If we replace x with 0, y with 1 and z with 2, we get words on the alphabet $\{0,1,2\}$ of length with i 0s, j 1s and k 2s.

(2) $F(1,1,1)=3^n$ counts the words of length n on the alphabet $\{0,1,2\}$.
- $F(-1,1,1)$ counts the words of length n on the alphabet $\{0,1,2\}$, but the coefficient $a_{i,j,k}$ is negative when i is odd.
- $F(1,-1,1)$ counts the words of length n on the alphabet $\{0,1,2\}$, but the coefficient $a_{i,j,k}$ is negative when j is odd.
- $F(-1,-1,1)$ counts the words of length n on the alphabet $\{0,1,2\}$, but the coefficient $a_{i,j,k}$ is negative when i is even and j is odd and when i is odd and j is even.
- In the sum $F(1,1,1)+F(-1,1,1)+F(1,-1,1)+F(-1,-1,1)$, the coefficients representing the words with an even number of 0s and an even number of 1s are positive in each summand, so they are counted four times. The coefficients representing the words with an odd number of 0s and an even number of 1s have positive sign in $F(1,1,1)$, negative sign in $F(-1,1,1)$, positive sign in $F(1,-1,1)$ and negative sign in $F(-1,-1,1)$, so they sum to zero. The same happens for the coefficients representing the words with an odd number of 0s and an even number of 1s. The coefficients representing the words with an odd number of 0s and an odd number of 1s are counted with a positive sign in $F(1,1,1)$, negative sign in $F(-1,1,1)$ and $F(1,-1,1)$ and a positive sign in $F(-1,-1,1)$, so they sum to zero. The only coefficients surviving is therefore the ones representing the words with an even number of 0s and an even number of 1s. We divide by 4 to get the correct number.

(3)

$$\begin{aligned}\sum_{n=0}^{\infty} b_n z^n &= \sum_{n=0}^{\infty} \frac{1}{4}(3^n+1^n+1^n+(-1)^n)z^n \\ &= \frac{1}{4}\left(\frac{1}{1-3z}+\frac{1}{1-z}+\frac{1}{1-z}+\frac{1}{1+z}\right) \\ &= \frac{1-2z-z^2}{1-3z-z^2+3z^3}.\end{aligned}$$

We use the generating function to find the recurrence relation.

$$\begin{aligned}B(z)(1-3z-z^2+3z^3) &= 1-2z-z^2 \\ B(z) &= 1-2z-z^2+3zB(z)+z^2B(z)-3z^3B(z) \\ &= 1-2z-z^2+3z\sum_{n=0}^{\infty} b_n z^n + z^2\sum_{n=0}^{\infty} b_n z^n - 3z^3\sum_{n=0}^{\infty} b_n z^n \\ &= 1-2z-z^2+\sum_{n=1}^{\infty} 3b_{n-1}z^n + \sum_{n=2}^{\infty} b_{n-2}z^n - \sum_{n=3}^{\infty} 3b_{n-3}z^n\end{aligned}$$

$$= 1 - 2z - z^2 + 3b_0 z + 3b_1 z^2 + b_0 z^2 + \sum_{n=3}^{\infty} 3b_{n-1} z^n + \sum_{n=3}^{\infty} b_{n-2} z^n - \sum_{n=3}^{\infty} 3b_{n-3} z^n$$

$$= 1 + (-2 + 3b_0)z + (-1 + 3b_1 + b_0)z^2 + \sum_{n=3}^{\infty} 3b_{n-1} + b_{n-2} - 3b_{n-3}$$

We have $a_n = 3b_{n-1} + b_{n-2} - 3b_{n-3}$ for $n \geq 3$ and $b_0 = 1$, $b_1 = -2 + 3b_0 = -2 + 3 = 1$ and $b_2 = -1 + 3b_1 + b_0 = -1 + 3 + 1 = 3$.

Problem 4.7. Give formulas for the generating function and the exponential generating function for the sequence $a_n = 2^n + 5^n$.

Solution.

$$\begin{aligned}
\sum_{n=0}^{\infty} a_n z^n &= \sum_{n=0}^{\infty} (2^n + 5^n) z^n \\
&= \sum_{n=0}^{\infty} (2z)^n + (5z)^n \\
&= \sum_{n=0}^{\infty} (2z)^n + \sum_{n=0}^{\infty} (5z)^n \\
&= \frac{1}{1-2z} + \frac{1}{1-5z} \\
&= \frac{2 - 7z}{1 - 7z + 10z^2}.
\end{aligned}$$

$$\begin{aligned}
\sum_{n=0}^{\infty} \frac{a_n}{n!} z^n &= \sum_{n=0}^{\infty} \frac{2^n + 5^n}{n!} z^n \\
&= \sum_{n=0}^{\infty} \frac{(2z)^n}{n!} + \frac{(5z)^n}{n!} \\
&= \sum_{n=0}^{\infty} \frac{(2z)^n}{n!} + \sum_{n=0}^{\infty} \frac{(5z)^n}{n!} \\
&= e^{2z} + e^{5z}.
\end{aligned}$$

Problem 4.8. Recall the Bell numbers from Problem 1.3. Using the recursive formula proven there for $\tilde{B}_{n+1}$, show that the exponential generating function $\hat{B}(z)$ for $\tilde{B}_n$ satisfies:

$$\frac{d\hat{B}(z)}{dz} = e^z \hat{B}(z).$$

Verify that $\hat{B}(z) = e^{e^z - 1}$ satisfies the above differential equation and that the first 3 terms of the series expansion of $e^{e^z - 1}$ give $\frac{\tilde{B}_i}{i!}$ for $i = 0, 1, 2$.

Solution.

$$\begin{aligned}\hat{B}(z) = \sum_{n=0}^{\infty} \frac{\tilde{B}_n}{n!} z^n &= \frac{\tilde{B}_0}{0!} z^0 + \sum_{n=0}^{\infty} \frac{\tilde{B}_{n+1}}{(n+1)!} z^{n+1} \\ &= 1 + \sum_{n=0}^{\infty} \frac{1}{(n+1)!} \sum_{k=0}^{n} \binom{n}{k} \tilde{B}_{n-k} z^{n+1}.\end{aligned}$$

$$\begin{aligned}\frac{d\hat{B}(z)}{dz} &= \sum_{n=0}^{\infty} \frac{n+1}{(n+1)!} \sum_{k=0}^{n} \binom{n}{k} \tilde{B}_{n-k} z^n \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} \tilde{B}_{n-k} z^n.\end{aligned}$$

$$\begin{aligned}e^z \hat{B}(z) &= \sum_{n=0}^{\infty} \frac{1}{n!} z^n \sum_{n=0}^{\infty} \frac{\tilde{B}_n}{n!} z^n \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{1}{k!} \frac{\tilde{B}_{n-k}}{(n-k)!} z^n,\end{aligned}$$

where we have used the multiplication rule.

Since

$$\frac{1}{n!} \binom{n}{k} = \frac{1}{n!} \frac{n!}{k!(n-k)!} = \frac{1}{k!(n-k)!},$$

we have that $\frac{d\hat{B}(z)}{dz} = e^z \hat{B}(z)$.

Let $\hat{B}(z) = e^{e^z - 1}$. Then

$$\begin{aligned}\frac{d\hat{B}(z)}{dz} &= \frac{d(e^{e^z-1})}{dz} \\ &= e^z \cdot e^{e^z - 1} \\ &= e^z \hat{B}(z).\end{aligned}$$

Since $\hat{B}(z) = e^{e^z - 1}$ satisfies the differential equation, we also have that

$$e^{e^z - 1} = \sum_{n=0}^{\infty} \frac{\tilde{B}_n}{n!} z^n,$$

where $\tilde{B}_n$ are the Bell numbers. We show this explicitly for $n = \{0, 1, 2\}$. Recall that the Taylor series expansion of $\hat{B}(z) = \sum_{n=0}^{\infty} \frac{\hat{B}(z)^{(n)}}{n!} z^n$ and that $\tilde{B}_0 = 1, \tilde{B}_1 = 1, \tilde{B}_2 = 2$.

$$\begin{aligned}\frac{e^{e^0-1}}{0!} &= 1 = \frac{\tilde{B}_0}{0!} \\ \frac{e^0 \cdot e^{e^0-1}}{1!} &= 1 = \frac{\tilde{B}_1}{1!} \\ \frac{e^0 e^{e^0-1} + e^0 e^0 e^{e^0-1}}{2!} &= 1 = \frac{\tilde{B}_2}{2!}\end{aligned}$$

Week of 17 Feb - Inclusion-exclusion and asymptotic analysis

Inclusion-exclusion, warm-ups.

(1) In a class of 50 students, 25 of the students study English, 20 study French, and 15 study German. Furthermore, 10 students study both English and French, 8 study both English and German, 5 study both French and German, and 3 study all three languages. How many students do not study any of the three languages?
(2) In how many ways can you arrange the digits $1, 2, 3, 4, 5$ such that 1 is not directly to the left of 2 and 2 is not directly to the left of 3? E.g. 13245 is allowed, 3**12**54 and 514**23** is not.
(3) What is the number of permutations on the set $\{1, \dots, 4\}$ with k fixed points for $k = 0, 1, 2, 3, 4$?
(4) Use inclusion-exclusion to find how many words on the alphabet 0,1,2 of length 5 contain each number at least once.
(5) How many of the numbers from 1 to 18 are divisible by either 2 or 3? How many of the numbers from 1 to 42 are not divisible by either 2, 3 or 7?

Solution.

(1) We use the Inclusion-Exclusion Principle and get
$$50 - 25 - 20 - 15 + 10 + 8 + 5 - 3 = 10.$$
(2) Let E_1 is the property that 1 is directly to left of 2 and E_2 the property that 2 is directly to left of 3. Then
$$\begin{aligned}\bar{N} &= 5! - N(E_1) - N(E_2) + N(E_1, E_2)\\ &= 5! - 4! - 4! + 3!\\ &= 120 - 24 - 24 + 6\\ &= 78.\end{aligned}$$
(3) $k = 4$: 1 (1234).
$k = 3$ 0 (if three are fixed, then all four are fixed)
$k = 2$ $\binom{4}{2} = 6$ (there is one permutation with 2 fixed points for every pair you pick).
$k = 0$:
$$\begin{aligned}\bar{N} &= 4! - \binom{4}{1}3! + \binom{4}{2}2! - \binom{4}{3}1! + \binom{4}{4}0!\\ &= 4! - 4 \cdot 3! + 6 \cdot 2! - 4 + 1\\ &= 9.\end{aligned}$$
$k = 1$:
$$\begin{aligned}\bar{N} = 4! &- |\text{exactly 4 fixed points}| - |\text{exactly 3 fixed points}|\\ &- |\text{exactly 2 fixed points}| - |\text{exactly 0 fixed points}|\\ &= 24 - 1 - 0 - 6 - 9\\ &= 8\end{aligned}$$
(4)
$$\binom{3}{0}3^5 - \binom{3}{1}2^5 + \binom{3}{2}1^5 - \binom{3}{3}0^3 = 3^5 - 3 \cdot 2^5 + 3 = 150,$$

where we first subtract the number of words with two or fewer letters, add the words with only one (or fewer) letter(s) and then subtract the number of words with zero letters (which is zero).

(5) Let E_1 be the numbers between 1 and 18 that are divisible by 2 and E_2 the numbers between 1 and 18 that are divisible by 3.

$$\begin{aligned}\bar{N} &= 18 - N(E_1) - N(E_2) + N(E_1, E_2)\\ &= 18 - \frac{18}{2} - \frac{18}{3} + \frac{18}{6}\\ &= 18 - 9 - 6 + 3\\ &= 6\end{aligned}$$

So there are $18 - 6 = 12$ numbers from 1 to 18 that are divisible by either 2 or 3. Let E_1 and E_2 be as before, but for the numbers between 1 and 42 and let E_3 be the numbers between 1 and 42 that are divisible by 7.

$$\begin{aligned}\bar{N} &= 42 - N(E_1) - N(E_2) - N(E_3) + N(E_1, E_2)\\ &\quad + N(E_1, E_3) + N(E_2, E_3) - N(E_1, E_2, E_3)\\ &= 42 - \frac{42}{2} - \frac{42}{3} - \frac{42}{7} + \frac{42}{6}\\ &\quad + \frac{42}{14} + \frac{42}{21} - \frac{42}{42}\\ &= 42 - 21 - 14 - 6 + 7 + 3 + 2 - 1\\ &= 12\end{aligned}$$

Problem 5.1. Let E be the set of maps $\phi : \{1, \dots, n\} \to \{1, \dots, r\}$. For an $m \in \{1, \dots, r\}$, let $E_m \subset E$ be the set of maps ϕ which do not hit m, i.e. of maps ϕ such that $\phi(k) \neq m$ for $k = 1, \dots, n$.

(1) Show that a map ϕ is surjective if and only if it does not lie in E_m for any $m \in \{1, \dots r\}$.

(2) Prove that

$$|E_m| = (r-1)^n.$$

(3) If $m_1, m_2, \dots, m_k \in \{1, \dots, r\}$ are distinct, prove that

$$|E_{m_1} \cap E_{m_2} \cap \cdots \cap E_{m_k}| = (r-k)^n.$$

(4) Prove using inclusion-exclusion that the number of surjective maps from $\{1, \dots, n\}$ to the set $\{1, \dots, r\}$ is

$$\sum_{k=0}^{r} (-1)^k \binom{r}{k} (r-k)^n$$

(5) Deduce that

$$S_{n,r} = \sum_{k=0}^{r} \frac{(-1)^k (r-k)^n}{k!(r-k)!}$$

Solution.

(1) Assume ϕ is surjective and let $m \in \{1, \dots, r\}$. Since ϕ is surjective, there exists an $k \in \{1, \dots, n\}$ such that $\phi(k) = m$. This means that ϕ does not lie in E_m. Assume now that ϕ does not lie in E_m for any $m \in \{1, \dots, r\}$. This means that for every $m \in \{1, \dots, r\}$ there exists a $k \in \{1, \dots, n\}$ such that $\phi(k) = m$, in other words: ϕ is surjective.

(2) The maps ϕ in E_m do not hit m, but can hit every other element in $\{1, \dots, r\}$. There are $(r-1)$ other elements which can be hit by each element in $\{1, \dots, n\}$, so the number of such maps is $(r-1)^n$.

(3) Since $m_1, m_2, \dots, m_k$ are distinct, $|E_{m_1} \cap E_{m_2} \cap \cdots \cap E_{m_k}|$ is the number of maps that do not hit $m_1, m_2, \dots, m_k$. The remaining $r-k$ can be hit by each element in $\{1, \dots, n\}$, so the number of maps is $(r-k)^n$.

(4) We proved in (1) that ϕ is surjective if and only if it does not lies in E_m for any $m \in \{1, \dots, r\}$. Let $\hat{N}$ denote the number of surjective maps. We have from Theorem 2.3 in Aigner that

$$|E \setminus \bigcup_{i=1}^{r} E_{m_i}| = |E| - \sum_{i=1}^{r} |E_{m_i}| + \sum_{0 \le i < j \le r} |E_{m_i} \cap E_{m_j}| - \cdots + (-1)^r |E_{m_1} \cap \cdots \cap E_{m_r}|$$

We use the results from (2) and (3) and get

$$\begin{aligned} |E \setminus \bigcup_{i=1}^{r} E_{m_i}| &= r^n - r(r-1)^n + \binom{r}{2}(r-2)^n - \cdots + (-1)^r \binom{r}{r}(r-r)^n \\ &= \sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^n \end{aligned}$$

(5) We use the facto from Aigner p.13 that the number of surjective maps from $\{1, \dots, n\}$ to $\{1, \dots, r\}$ is $r! S_{n,r}$. Then

$$\begin{aligned} S_{n,r} &= \frac{1}{r!} \sum_{i=0}^{r} (-1)^i \binom{r}{i} (r-i)^n \\ &= \sum_{i=0}^{r} (-1)^i \frac{1}{r!} \frac{r!}{i!(r-i)!} (r-i)^n \\ &= \sum_{i=0}^{r} (-1)^i \frac{(r-i)^n}{i!(r-i)!} \end{aligned}$$

Problem 5.2. Let $\phi(n)$ denote the number of integers k such that $1 \le k \le n$ and k is relatively prime to n. Prove using inclusion-exclusion that

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right),$$

where $n = p_1^{l_1} p_2^{l_2} \dots p_t^{l_t}$

Solution. We use the same approach as in warm up (5). Let E_i be the numbers between 1 and k that are divisible by p_i. We use Theorem 2.4 in Aigner and get

$$\begin{aligned}\phi(n) &= n - \sum_{i=1}^{t} N(E_i) + \sum_{1\le i<j\le t} N(E_i, E_j) - \cdots + (-1)^t N(E_1, \dots E_t) \\ &= n - \frac{n}{p_1} - \cdots - \frac{n}{p_t} + \sum_{1\le i<j\le t} \frac{n}{p_i p_j} - \cdots + (-1)^t \frac{n}{p_1 \dots p_t} \\ &= n\left(1 - \frac{1}{p_1} - \cdots - \frac{1}{p_t} + \sum_{1\le i<j\le t} \frac{1}{p_i p_j} - \cdots + (-1)^t \frac{1}{p_1 \dots p_t}\right) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_t}\right).\end{aligned}$$

Asymptotic analysis, warm-ups.

(1) Order the following functions by the relation $\prec$.
$$e^n, n^n, \log(2n), n, 2, 2^n, \log(n), n^2, n!$$
(2) Let $f_1(n) = n, f_2(n) = n^2, g_1(n) = n^3 + n$ and $g_2(n) = -n^3$. Show that
$$f_1(n) \prec g_1(n), f_2(n) \prec g_2(n),$$
but that we do not have
$$f_1(n) + f_2(n) \prec g_1(n) + g_2(n).$$
(3) Find an example of two polynomials $f(n)$ and $g(n)$ such that $f(n) < g(n)$ for all n, but such that we do not have
$$f(n) \prec g(n).$$
(4) If an algorithm for an input of length n executes n steps where the ith step requires 2 operations, what is the Big-O running time of the algorithm?
(5) If an algorithm for an input of length n executes n steps where the ith step requires n^2 operations, what is the Big-O running time of the algorithm?

Solution.

(1) We follow the arguments in Aigner p. 100 and get
$$2 \prec \log(n) \prec \log(2n) \prec n \prec n^2 \prec 2^n \prec e^n \prec n! \prec n^n$$
(2) We have
$$\lim_{n\to\infty} \frac{f_1(n)}{g_1(n)} = \lim_{n\to\infty} \frac{n}{n^3 + n} = \lim_{n\to\infty} \frac{1}{n^2 + 1} = 0,$$
$$\lim_{n\to\infty} \left|\frac{f_2(n)}{g_2(n)}\right| = \lim_{n\to\infty} \frac{n^2}{n^3} = \lim_{n\to\infty} \frac{1}{n} = 0,$$
$$\lim_{n\to\infty} \frac{f_1(n) + f_2(n)}{g_1(n) + g_2(n)} = \lim_{n\to\infty} \frac{n + n^2}{n^3 + n - n^3} = \lim_{n\to\infty} \frac{n + n^2}{n} = \lim_{n\to\infty} \frac{1 + n}{1} = \infty$$
(3) Let $f(n) = n$ and $g(n) = n + 1$. Then $f(n) = n < n + 1 = g(n)$ for all n, but
$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \lim_{n\to\infty} \frac{n}{n + 1} = 1.$$

(4) The total number of operations is $2 \cdot n = 2n$. We want to show that $2n = O(n)$ in the notation of Aigner.

$$O(n) = \{f(n) : \text{there exists a constant } C \geq 0 \text{ such that } |f(n)| \leq Cn \text{ for } n \geq n_0\}$$

If we let $C = 2$, we have that $2n \leq 2 \cdot n$, so $2n = O(n)$. The Big-O running time for the algorithm is therefore $O(n)$.

(5) The total number of operations is $n \cdot n^2 = 3$ and the Big-O running time for the algorithm is $O(n^3)$.

Problem 5.3.

(1) Show that

$$n^n \leq (n!)^2 \quad \text{for } n \geq 1. \tag{A}$$

Hint: First use

$$k(n+1-k) = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n+1}{2} - k\right)^2$$

to show that for $1 \leq k \leq n$, we have

$$k(n+1-k) \geq n.$$

(2) Use Stirling's formula for the asymptotics of $n!$ to show that

$$n^n \prec (n!)^2. \tag{B}$$

Explain why (A) does not imply (B).

Solution.

(1) We have that $\frac{n+1}{2} - k$ increases when k increases from 1 to n, and that $\frac{n+1}{2} - 1 = -(\frac{n+1}{2} - n) =$. This means that $\left(\frac{n+1}{2} - k\right)^2 \leq \left(\frac{n+1}{2} - 1\right)^2 = \left(\frac{n-1}{2}\right)^2$. We therefore have

$$k(n+1-k) = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n+1}{2} - k\right)^2 \geq \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = n.$$

Now we show that

$$n^n \leq (n!)^2 \quad \text{for } n \geq 1.$$

$$\begin{aligned}(n!)^2 &= (n \cdot (n-1) \cdot \ldots 2 \cdot 1)(n \cdot (n-1) \cdot \cdots \cdot 2 \cdot 1) \\ &= (1 \cdot n)(2 \cdot (n-1)) \cdot \cdots \cdot ((n-1) \cdot 2)(n \cdot 1) \\ &\geq n^n,\end{aligned}$$

where we have used that each factor in the second line is on the form $k(n+1-k)$ for $1 \leq k \leq n$.

(2) Stirling's formula says that $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$, so

$$\begin{aligned}\lim_{n\to\infty}\frac{n^n}{(n!)^2} &= \lim_{n\to\infty}\frac{n^n}{\left(\sqrt{2\pi n}\left(\frac{n}{e}\right)^n\right)^2}\\ &= \lim_{n\to\infty}\frac{n^n}{2\pi n\cdot n^{2n}e^{-2n})}\\ &= \lim_{n\to\infty}\frac{(e^2)^n}{2\pi n\cdot n^n}\\ &= 0,\end{aligned}$$

since n^n goes to zero faster than $(e^2)^n$ goes to zero.

(A) does not imply (B) since we do not know from (A) how fast n^n and $(n!)^2$ change.

Problem 5.4. Use Stirling's formula to show

$$\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi n}}.$$

Get a sense of the accuracy of this asymptotic estimate by computing

$$\frac{\binom{2n}{n}}{4^n/\sqrt{\pi n}}$$

as a decimal number for $n = 1, 10, 100, 1000$, and by plotting the graph of this expression as a function of n.

Solution.

$$\binom{2n}{n} = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{(n!)^2}$$

We use Stirling's formula on both $(2n)!$ and $(n!)^2$.

$$\begin{aligned}\lim_{n\to\infty}\frac{(2n)!(n!)^{-2}}{4^n/\sqrt{\pi n}} &= \lim_{n\to\infty}\frac{\sqrt{2\pi(2n)}(2n)^{2n}e^{-2n}\cdot(2\pi n)^{-1}n^{-2n}e^{2n}}{4^n/\sqrt{\pi n}}\\ &= \lim_{n\to\infty}\frac{2\sqrt{\pi n}4^n n^{2n}e^{2n-2n}n^{-2n}}{(2\pi n)4^n/\sqrt{\pi n}}\\ &= \lim_{n\to\infty}\frac{2\cdot\pi n}{2\pi n}\\ &= 1\end{aligned}$$

$n = 1$: 0,282
$n = 10$: 0,0314
$n = 100$: 0,0032
$n = 1000$: 0,00031.

Problem 5.5. Let $f, g : \mathbb{N} \to \mathbb{R}$ be positive functions. Prove that if $h(n) \in O(f(n))$ and $j(n) \in O(g(n))$, then

(1) $h(n)j(n) \in O(f(n)g(n))$
(2) $h(n) + j(n) \in O(f(n) + g(n))$.

Solution. Since $h(n) \in O(f(n))$, there exists a constant $C > 0$ such that $|h(n)| \leq C|f(n)|$ for $n \geq n_0$, and since $j(n) \in O(g(n))$, there exists a constant $C' > 0$ such that $|j(n)| \leq C'|g(n)|$ for $n \geq n_0'$.

(1) We have that $h(n)j(n) \in O(f(n)g(n))$ if there exists a constant $D > 0$ such that $|h(n)j(n)| \leq D|f(n)g(n)|$ for $n \geq m_0$. Indeed, we have

$$\begin{aligned} |h(n)j(n)| &= |h(n)||j(n)| \\ &\leq C|f(n)|C'|g(n)| \\ &= CC'|f(n)g(n)|, \end{aligned}$$

for $n \geq m_0$, where $m_0 = \max\{n_0, n_1'\}$.

(2) In the same way, we have that $h(n) + j(n) \in O(f(n) + g(n))$ if there exists a constant $D' \geq 0$ such that $|h(n) + j(n)| \leq D'|f(n) + g(n)|$ for $n \geq m_0'$. Indeed, we have

$$\begin{aligned} |h(n) + j(n)| &\leq |h(n)| + |j(n)| \\ &\leq C|f(n)| + C'|g(n)| \\ &\leq \max\{C, C'\}(|f(n)| + |g(n)|) \\ &= \max\{C, C'\}|f(n) + g(n)|, \end{aligned}$$

where the last equality follow since f, g are positive functions.

Week of 24 Feb - Graph theory

Warm ups.

(1) How many edges are there in the complete graph on n vertices.
(2) Is there a 3-regular graph on 5 vertices?
(3) Write down the adjacency and incidence matrices for the complete graph on 4 vertices.
(4) Write down the adjacency and incidence matrices for a labeling of the circuit graph on 4 vertices.
(5) Write down the adjacency and incidence matrices for the hypercube graph Q_2.

Solution.

(1) In a complete graph, there are edges between every pair of vertices, so the number is $\binom{n}{2}$.
(2) A complete graph of 5 vertices has $\binom{5}{2} = 10$ edges, but a 3-regular graph on 5 vertices should have $3 \cdot 5 = 15$ edges, so it is not possible.
(3) **Adjacency matrix**:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Incidence matrix: There are 4 vertices and $\binom{4}{2} = 6$ edges, so the incidence matrix is a 4×6-matrix. We number the edges in the following way:

$$e_1 = (v_1, v_2)$$
$$e_2 = (v_1, v_3)$$
$$e_3 = (v_1, v_4)$$
$$e_4 = (v_2, v_3)$$
$$e_5 = (v_2, v_4)$$
$$e_6 = (v_3, v_4)$$

Then the matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(4) We label the vertices in a cyclic order and the edges in the following way:

$$e_1 = (v_1, v_2)$$
$$e_2 = (v_2, v_3)$$
$$e_3 = (v_3, v_4)$$
$$e_4 = (v_4, v_1)$$

Adjacency matrix:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

(5) We label the vertices the following way: $v_1 = 00, v_2 = 01, v_3 = 10, v_4 = 11$. We label the edges in the following way:

$$e_1 = (v_1, v_2)$$
$$e_2 = (v_1, v_3)$$
$$e_3 = (v_2, v_4)$$
$$e_4 = (v_3, v_4)$$

Adjacency matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Incidence matrix:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

Problem 6.1. Show that a graph with $n \geq 2$ vertices has at least two vertices of the same degree. *Hint: The degree $d(v)$ of a vertex v must satisfy $0 \leq d(v) \leq n-1$. If there is a vertex of degree $n-1$, can there be a vertex of degree 0?*

Solution. We follow the hint and use the fact that the degree of the vertex is between 0 and $n-1$. We divide the problem into two cases:

- Case 1: No vertex has degree 0. Then the possible degrees are 1 to $n-1$, i.e. there are $n-1$ possibilities for the n vertices. By the Pigeonhole Principle, at least two vertices must have the same degree.
- Case 2: There is a vertex of degree 0. Then no vertex can have degree $n-1$, so the possible degrees for the remaining vertices are between 0 and $n-2$. By the Pigeonhole Principle, at least two vertices must have the same degree.

Problem 6.2. Which of the graphs K_n, P_n, C_n, Q_n are bipartite? The answer may depend on n.

Solution.

- K_n: K_1 and K_2 are bipartite. For $n \geq 3$, there are loops of odd length, so K_n is not bipartite.
- P_n: We let S be the vertices with odd indices and let T be the vertices with even indices, and see that P_n is bipartite for every n.
- C_n: When n is even, we choose S and T as for P_n and we see that C_n are bipartite. When n is odd, v_1 and v_n are both in S, but are adjacent, so the graph is not bipartite.
- Q_n: We let S be the vertices with an odd number of 1s and let T be the vertices with an even number of 1s. Since adjacent vertices differ by one bit, they will have different parity of 1s.

Problem 6.3. A k-colouring of a graph $G = (V, E)$ is an assignment $f : V \to C$ where $|C| = k$ and such that $uv \in E$ implies $f(u) \neq f(v)$ (imagine that C is considered a set of colours, and we ask for ways to colour the vertices so that adjacent vertices have different colours).

(1) Prove that G has a 1-colouring if and only if $E = \emptyset$
(2) Prove that G has a 2-colouring if and only if G is bipartite.
(3) Show that the number of k-colourings of
   (a) the complete graph K_n is $\binom{k}{n}$.
   (b) the path graph P_n is $k(k-1)^{n-1}$.
   (c) the circuit graph C_n is

$$\sum_{i=0}^{n-1} (-1)^i \binom{n}{i} k^{n-i} + (-1)^n k$$

Hint: Use the inclusion-exclusion principle on the set of colour functions $f : V \to C$ and, for each edge uv, the subset E_{uv} of functions where $f(u) = f(v)$.

Solution.

(1) If $E = \emptyset$, G obviously has a 1-colouring since $f(u) \neq f(v)$ for $uv \in E$ is trivially fulfilled. Assume G has a 1-colouring. Then $f(v) = c$ for every $v \in V$. Further, we have that for $uv \in E$, $f(u) \neq f(v)$. Since $f(v) = f(u)$ for every $u, v \in V$, $E = \emptyset$.

(2) Assume G has a 2-colouring. Since $f(u) \neq f(v)$ for $uv \in E$, we can use the colouring to divide the vertices into sets S and T, where each edge has one vertex in S and one in T. Assume that G is bipartite. Then we have S and T such that each edge has one vertex in S and one vertex in T. If we let $f(v) = c$ for $v \in S$ and $f(v) = d$ for $v \in T$. Then f is a 2-colouring of G.

(3) (a) Since every vertex is adjacent to every other vertex, we must have different colours on each vertex. For the first vertex there are k possibilities, $k - 1$ for the next and $k - (n - 1)$ for the last. This gives

$$k \cdot (k-1) \cdot \cdots \cdot (k-n+1) = \binom{k}{n}$$

possibilities.

(b) For the first vertex there are k possibilities. The next vertex is adjacent to the first, so there are $k - 1$ possibilities. The third is adjacent to the second, but not to the first, so there are $k - 1$ possibilities. The same happens for the rest of the vertices, so there are $k(k-1)^{n-1}$ possibilities.

(c) We follow the hint and let E_{uv} be the set of functions $f : V \to C$ such that $f(u) = f(v)$. We want to find the number of functions such that $f(u) \neq f(v)$ for $uv \in E$, i.e. the number of functions that do not belong to any of the E_{uv}. To make write the sum easier, we write E_i. The total number of k-colourings is k^n and by the inclusion-exclusion principle we get

$$\bar{N} = k^n - \sum_{i=1}^{n} N(E_i) + \sum_{1 \leq i < j \leq n} N(E_i E_j) - \cdots + (-1)^n N(E_1 \dots E_n).$$

We investigate the term $\sum_{i=1}^{n} N(E_i)$. For each edge, if the endpoints should have the same colour, there are k possibilities. The rest of the $n - 2$ vertices can also have each of the k colour, thus there are $k \cdot k^{(n-2)} = k^{(n-1)}$ colourings. This gives that

$$\sum_{i=1}^{n} N(E_i) = nk^{(n-1)}.$$

Let us now investigate the terms $\sum_{1 \leq i < j \leq n} N(E_i E_j)$. If the two edges share a vertex, then three vertices must have the same colour, k possibilities, and the remaining $(n-3)$ can have each of the k colours. Thus, $k \cdot k^{(n-3)} = k^{(n-2)}$ colourings for edges that share a vertex. If the two edges do not share a vertex, then we have k possibilities for the endpoints of the first edge, k possibilities for the endpoints of the second edge and k possibilities for the remaining $n - 4$ vertices. This gives

$k \cdot k \cdot k^{(n-4)} = k^{(n-2)}$ colourings. In either case we get $k^{(n-2)}$ possibilities. There are $\binom{n}{2}$ pairs of edges, so $\sum_{1 \leq i < j \leq n} N(E_i E_j) = \binom{n}{2} k^{(n-2)}$.

The same happens for 3 edges etc. up to $n-1$ edges. For $N(E_1 \dots E_n)$ we get k possibilities. This gives the sum

$$\begin{aligned} \bar{N} &= k^n + \sum_{i=1}^{n-1} (-1)^i \binom{n}{i} k^{n-i} + (-1)^n k \\ &= \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} k^{n-i} + (-1)^n k. \end{aligned}$$

Problem 6.4. A **cut edge** k of a graph $G = (V, E)$ is an edge such that the graph $(V, E - k)$ has more components than G.

(1) Which of the graphs K_n, C_n and P_n, and the Peterson graph have a cut edge?
(2) If k is the edge between the vertices u and v, show that k is a cut edge if and only if there is no path connecting u and v which does not contain k.
(3) Show that k is a cut edge if and only if it is not contained in a circuit.

Solution.

(1)
- K_1 has no edges, so it has no cut edges. K_2 has one edge, which is a cut edge. K_n for $n \geq 3$ has no cut edges since every vertex has degree $n - 1$.
- Removing one edge from C_n will turn the graph into a path, which is connected, so C_n has no cut edges.
- P_1 has no edges, so it has no cut edges. For K_n for $n \geq 2$ every edge is a cut edge.
- In the Petersen graph, every vertex has degree 3, therefore it has no cut edges.

(2) Assume k is a cut edge. Assume for contradiction that there is a path connecting u and v which does not contain k. However, since k is a cut edge, removing k will disconnect the graph. Since k was an edge between u and v, u and v must be in different components after removing k. This contradicts the fact that there is a path connecting u and v not containing k. For the opposite direction, assume that there is no path connecting u and v that does not contain k and remove k. Then there is no path between u and v, so u and v are in different components. This shows that k is a cut edge.

(3) Assume k is a cut edge. Assume for contradiction that k is contained in a circuit. Since k is in a circuit, removing k will still connect the endpoints of k. This contradicts the fact that k is a cut edge. For the opposite direction, assume that k is not in a circuit. Since k is not in a circuit, removing k will disconnect the endpoints of k, making the graph disconnected. Thus, k is a cut edge.

Problem 6.5. Let G be a graph, and let v be a vertex. Let $G - v$ be the graph obtained by deleting v and all edges incident to v. We say v is a **cut vertex** if $G - v$ has more connected components than G.

Assume now that G is connected, that v is a cut vertex, and that $u \neq v$ is some other vertex.

(1) Prove that there exists a vertex w such that every path from u to w passes through v.
(2) Prove that for this w we have
$$d(u, w) = d(v, w) + d(v, u).$$
(3) Prove that $d(v, u) < D(G)$.
(4) Prove that G has at least two vertices which are not cut.

Solution.

(1) Assume G is connected, v is a cut vertex and that $u \neq v$ is some other vertex. Assume for contradiction that for every vertex w, there exists a path from u to w that do not pass through v. Let w be in another component than u in $G - v$. Since G is connected, there exists a path from u to w in G. Since v is a cut vertex and u and w are in different components in $G - v$, every path from u to w in G must pass through v.
(2) Let $d(u, w)$ denote the shortest path from u to w. Since every path from u to w passes through v, any shortest path must also pass through v. We decompose $d(u, w)$ into $d(v, w) + d(v, u)$, where $d(v, w)$ is the shortest path from v to w and $d(v, u)$ is the shortest path from v to u. If they were not a shortest paths, $d(u, v)$ would not be a shortest path either. This shows that $d(u, w) = d(v, w) + d(v, u)$.
(3) Recall that $D(G) = \max_{u,v \in V} d(u, v)$. We assumed $u \neq v$ and that w is in another component than w, thus $w \neq v$ and $d(v, w) > 0$. This gives
$$d(u, w) = d(v, w) + d(v, u) > d(v, u).$$
Since $d(v, u) < d(u, w)$, we have $d(v, u) < D(G)$.
(4) Let P be a longest path in G with endpoints u and v. We want to show that u and v are not cut vertices. Assume for contradiction that v is a cut vertex. Then $u \neq v$ is some other vertex. We have shown in (3) that $d(u, v) < D(G)$. This is a contradiction since we assumed u and v was the endpoints of a longest path in G. The argument is similar for u.

Problem 6.6. Assume a graph G has the property that every pair of edges are incident. Prove that then either

(1) There exists a vertex v so that every edge is incident to v, or
(2) There exist vertices u, v, w so that edges of G are uv, vw, uw.

Solution. If G fulfil (1) we obviously have that every pair of edges are incident (since they all are incident to v). Assume that G do not fulfil (1). We want to show that then G fulfil (2). Let e_1 and e_2 be two edges and such that u, v are the endpoints of e_1 and u, w are the endpoints of e_2. Since G do not fulfil (1) there must exists an edge e_3 which is not incident to u, but incident to both e_1 and e_2.

Thus, e_3 has endpoints v, w. Any fourth edge must be incident to e_1, e_2, e_3, but this is not possible.

Problem 6.7.

(1) Show that a 3-regular graph has an even number of vertices.
(2) Construct a 3-regular graph with 4 vertices.
(3) Use Problem 6.6 to show that a 3-regular graph has a pair of non-incident edges.
(4) Let G be a 3-regular graph, and let e, f be non-incident edges of G. Construct a new 3-regular graph from G by adding 2 vertices, deleting edges e, f, and adding 5 new edges.
(5) Prove by induction that for every even n, there exists a connected 3-regular graph with n vertices.

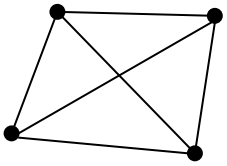
Solution.

(1) Recall Theorem 6.1 in Aigner, we says that

$$\sum_{u \in V} d(u) = 2|E|,$$

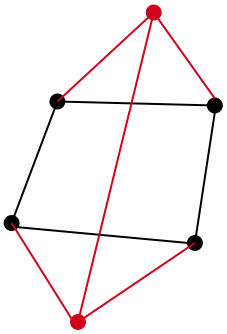
where $d(u)$ is the degree of a vertex u. We observer that the right side of the equation is always even. For a 3-regular graph, $d(u) = 3$ for all u. Thus, to get an even number on the left side of the equation, the number of vertices must be even.

(2) The graph:



(3) Assume for contradiction that every pair of edges in a 3-regular graph G are incident. Then G fulfil either (1) or (2) from Problem 6.6. If we are in case 1, then there exists a vertex v such that all edges are incident to v. Since G is 3-regular, there can only be three edges incident to v. But this is not a 3-regular graph, since the vertices which is the other endpoints of the three edges have degree 1. If we are in case 2, G is a triangle graph which is 2-regular, not 3-regular, so we have a contradiction.

(4) We let G be the 3-regular graph with 4 vertices.



(5) We have shown that there exists a 3-regular graph for $n = 4$. Assume that there exists a 3-regular graph for an even k. We want to prove that there exists a 3-regular graph with $k + 2$ vertices. The step from k to $k + 2$ is described in (4).

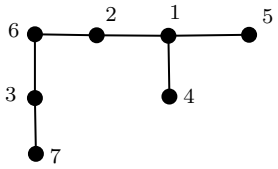
Week of 3 March - Trees

Warm-ups. The **Prüfer code** of a spanning tree of K_n is the sequence produced in the proof of Theorem 7.4.

(1) Draw the spanning tree of K_7 of the Prüfer code $(1, 1, 3, 2, 6)$.
(2) Find the Prüfer code of the path P_n labelled sequentially with $1, 2, \ldots, n$.
(3) How many edges must be removed from the hypercube graph to obtain a spanning tree?
(4) What trees do the breadth-first and depth-first searches return on K_n?
(5) What are the bases of the matroid of the circuit graph C_n?

Solution.

(1) We follow the steps given in the proof of Theorem 7.4:



(2) The edges of P_n are $(1, 2), (2, 3) \ldots (n-1, n)$ and the leaves are the vertices 1 and n. The smallest leaf is 1 with neighbour 2, so the first number in the Prüfer code is 2. Now, we remove 1, so the smallest leaf is 2 with neighbour 3. The next number in the Prüfer code is therefore 3. We continue in this way until we remove vertex $n - 2$. Then the remaining vertices are $n - 1$ and n, so the Prüfer code becomes $(2, 3, \ldots, n - 1)$.
(3) The hypercube Q_n has 2^n vertices, so there is $2^n - 1$ edges in a spanning tree. The number of edges in Q_n is $n2^{n-1}$ (page 121 in Aigner). Thus, we must remove $n2^{n-1} - (2^n - 1) = 2^{n-1}(n-2)+1$ edges to obtain a spanning tree.
(4)
- Let v be the start vertex. Since every vertex in K_n is a neighbour of v, we add the edges (vj) for all $j \in V/v$. The breath-first search therefore returns a star graph.
- Since there are edges between every pair of vertices the depth-first search returns a path graph.

(5) The bases of the matroid of the circiut graph C_n are the spanning trees. The spanning trees of C_n are all the path we get by deleting one edge of C_n.

Problem 7.1. Let $d_1, \ldots, d_n$ be natural numbers with $d_i \geq 1$ and

$$\sum_{i=1}^{n} d_i = 2n - 2$$

Show that the number of spanning trees of K_n with vertex i having degree d_i is equal to

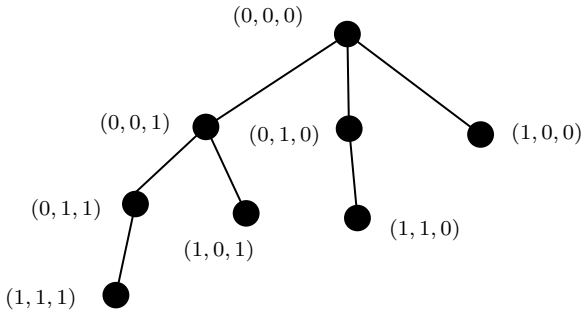
$$\frac{(n-2)!}{(d_1-1)!\dots(d_n-1)!}.$$

Solution. We show this by computing the number of Prüfer codes we can obtain by the given degrees. The Prüfer code has length $n-2$ and i appears d_i-1 times. Let N be the number of Prüfer codes. Then

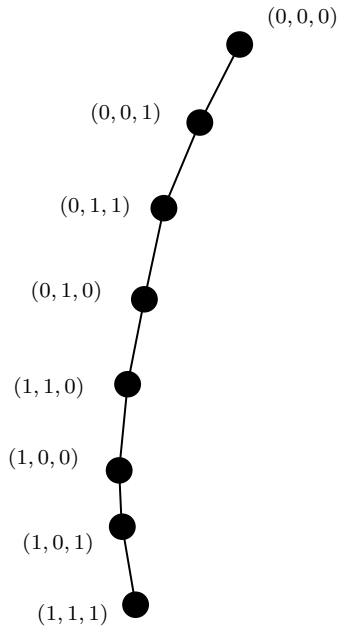
$$\begin{aligned} N &= \binom{n-2}{d_1-1}\binom{n-2-(d_1-1)}{d_2-1}\cdots\binom{n-2-\sum_{i=1}^{n}(d_i-1)}{d_n-1} \\ &= \frac{(n-2)!}{(d_1-1)!(n-2-(d_1-1)!)}\frac{(n-2-(d_1-1))!}{(d_2-1)!(n-2-(d_1-1)-(d_2-2))!}\cdots \\ &= \frac{(n-2)!}{(d_1-1)!(d_2-1)!\dots(d_n-1)!} \end{aligned}$$

Problem 7.2. Perform the depth-first search and breadth-first search algorithms on the hypercube graph Q_3 from starting vertex $(0,0,0)$ and describe the resulting trees.

Solution. The breadth-first search:



The depth-first search:



Problem 7.3. Label the vertices of K_n with $1, ..., n$ and consider the weight function given by $w(ij) = i + j$. Construct a minimal spanning tree T for this weight function. Is this tree unique? What is $w(T)$?

Solution. The edge of minimal weight is (12), so this is our first edge. Now, the next edge of minimal weight is (13). We continue in this way and choose the edges $(12), (13), (14), \dots (1, n)$. This creates a star shaped spanning tree where all edges are incident to the first vertex 1. We have used all the edges that are incident to 1. Choosing another edge would give a higher weight, so the spanning tree is unique.

$$w(T) = \sum_{i=2}^{n}(i+1) = \frac{n(n+1)}{2} - 1 + (n-1) = \frac{1}{2}(n^2 + 3n - 4).$$

1. Week of 10 March – Matchings, Eulerian and Hamiltonian circuits

Warm ups.

(1) Can you remove 3 edges from $K_{4,4}$ so that there is no longer a matching with $|M| = 4$?
(2) For what values of n is K_n Eulerian?
(3) For what values of n and m is $K_{n,m}$ Eulerian?

Solution.

(1) We use Theorem 8.3, which says that for a bipartite graph $G = (S + T, E)$, $m(G) = |S|$ if and only if $|A| \leq |N(A)|$ for all $A \subset S$, where $N(A) = \{v \in T : uv \in E \text{ for some } u \in A\}$. In $K_{4,4}$, every vertex in S is connected to every vertex in T. Therefore, $N(A) = 4|A|$ for every $A \subset S$. Removing 3 edges will at most reduce $N(A)$ by 3. Thus $\bar{N}(A) = 4|A| - 3$, which is greater than or equal to $|A|$ since we can have $|A| = 1, 2, 3, 4$. This

show that we cannot remove 3 edges from $K_{4,4}$ so that there is no longer a matching with $|M| = 4$.

(2) We use Theorem 8.19, which says that a graph $G \neq \emptyset$ is Eulerian if and only if G is is connected and all vertices has even degree. In K_n, every vertex has degree $n-1$, so K_n is Eulerian iff $n-1$ is even, that is when n is odd.

(3) In $K_{n,m}$ the first set of vertices has degree m and the second set has degree n. Since all vertices should have even degree, both m and n must be even.

Problem 8.1. Suppose a bipartite graph is k-regular for $k \geq 1$. Show that $|S| = |T|$ and that G contains a matching with $|M| = |S| = |T|$.

Solution. First, we show that $|S| = |T|$. Let E denote the set of edges. Since the graph is k-regular, $|E| = k|S|$ and $|E| = k|T|$. Thus, $|E| = k|S| = k|T|$ and get that $|S| = |T|$. Now, we show that G contains a matching with $|M| = |S| = |T|$. We use Theorem 8.3. Let A be any subset of S and let $E(A, N(A))$ be the set of edges between A and $N(A)$. Since G is k-regular, $E(A, N(A)) = k|A|$. Further, we have that $E(A, N(A)) \leq k|N(A)|$, since there can be more edges from $N(A)$ than does incident to vertices in A. Therefore, $k|A| = E(A, N(A)) \leq k|N(A)|$, which gives $|A| \leq |N(A)|$.

Problem 8.2. Use Algorithm 8.12 from the book to find a perfect matching of $K_{5,5}$ of minimal weight if the weight function on the edges is encoded by the matrix:

$$\begin{pmatrix} 8 & 7 & 5 & 11 & 4 \\ 9 & 7 & 6 & 11 & 3 \\ 12 & 9 & 4 & 8 & 2 \\ 1 & 2 & 3 & 5 & 6 \\ 11 & 4 & 2 & 8 & 2 \end{pmatrix}$$

Solution.

(1) Initialization:

(1) $p_1 = \min_j(w_{1j}) = 4$, $p_2 = \min_j(w_{2j}) = 3$, $p_3 = \min_j(w_{3j}) = 2$, $p_4 = \min_j(w_{4j}) = 1$, $p_5 = \min_j(w_{5j}) = 2$, so (w'_{ij}) becomes:

$$\begin{pmatrix} 4 & 3 & 1 & 7 & 0 \\ 6 & 4 & 3 & 8 & 0 \\ 10 & 7 & 2 & 6 & 0 \\ 0 & 1 & 2 & 4 & 5 \\ 9 & 2 & 0 & 6 & 0 \end{pmatrix}$$

$q_1 = \min_i(w'_{i1}) = 0$, $q_2 = \min_i(w'_{i2}) = 1$, $q_3 = \min_i(w'_{i3}) = 0$, $q_4 = \min_i(w'_{i4}) = 4$, $q_5 = \min_i(w'_{i5}) = 0$, so $(\bar{w}_{ij})$ becomes:

$$\begin{pmatrix} 4 & 2 & 1 & 3 & 0 \\ 6 & 3 & 3 & 4 & 0 \\ 10 & 6 & 2 & 2 & 0 \\ 0 & 0 & 2 & 0 & 5 \\ 9 & 1 & 0 & 2 & 0 \end{pmatrix}$$

(2) A minimal zero-covering in $(\bar{w}_{ij})$ is the fourth row and the third and fifth column. Since the covering contains fewer than 5 rows and columns, we go to step (3).
(3) We have that the smallest uncovered entry $\bar{w}$ is 1, so we subtract 1 from all uncovered entries and add 1 to all doubly covered entries. Then $(\bar{\bar{w}}_{ij})$ becomes:

$$\begin{pmatrix} 3 & 1 & 1 & 2 & 0 \\ 5 & 2 & 3 & 3 & 0 \\ 9 & 5 & 2 & 1 & 0 \\ 0 & 0 & 3 & 0 & 6 \\ 8 & 0 & 0 & 1 & 0 \end{pmatrix}$$

A minimal zero-covering is the fourth and fifth row and the fifth column. Since the covering contains fewer than 5 rows and columns, we continue on step (3). We have that the smallest uncovered entry $\bar{w}$ is 1, so we subtract 1 from all uncovered entries and add 1 to all doubly covered entries. Then $(\bar{\bar{w}}_{ij})$ becomes:

$$\begin{pmatrix} 2 & 0 & 0 & 1 & 0 \\ 4 & 1 & 2 & 2 & 0 \\ 8 & 4 & 1 & 0 & 0 \\ 0 & 0 & 3 & 0 & 7 \\ 8 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Now, we have to use 5 rows and columns to find a minimal zero-covering, so we go to step (4).
(4)

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

We get the matching

$$(1,2) = 7$$
$$(2,5) = 3$$
$$(3,4) = 8$$
$$(4,1) = 1$$
$$(5,3) = 2$$

Week of 17 March – More on matchings and the travelling salesman problem

Problem 9.1.

(1) For what values of n is the hypercube graph Q_n Eulerian?
(2) For $n \geq 2$, describe a Hamiltonian circuit in the hypercube graph Q_n.

Solution.

(1) We have from Theorem 8.19 that Q_n is Eulerian if and only if the vertices have even degree. Every vertex in Q_n as degree n, thus Q_n is Eulerian iff n is even.
(2) We prove this by induction. Q_4 is a Hambiltonial circuit. Assume there exists a Hamiltonian circuit C_n in Q_n. We find a Hamiltonian circuit C_{n+1} in Q_{n+1} in the following way. Do C_n, but omit the last step, in the part of Q_{n+1} where the first coordinate is 0 such that the final step is a neighbour of $(0,\dots,0)$. Then, change the first coordinate to 1, and do the circuit C_n in opposite direction so that we end up in $(1,0,\dots,0)$. The last step is $(1,0,\dots,0)$ to $(0,\dots,0)$.

Problem 9.2. Give an example of a bipartite graph G and a matching M with $|M| < m(G)$ such that there is no matching M' with $M \subsetneq M'$.

Solution. Let $S = \{u_0, u_1, u_2, u_3\}$ and $T = \{v_0, v_1, v_2, v_3\}$ with edges E

- (u_0, v_0)
- (u_1, v_1)
- (u_2, v_2)
- (u_2, v_3)
- (u_3, v_2)

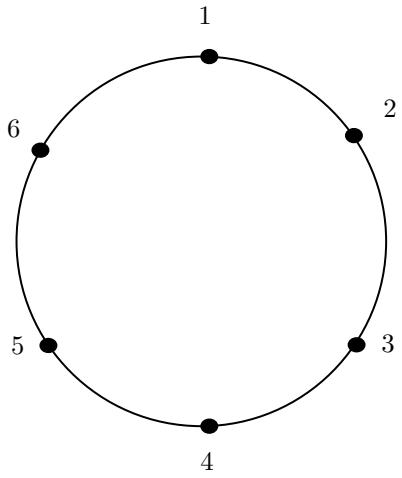
Then $G(S+T, E)$ is an example of such a graph (why?) (choose (u_0, v_0),(u_1, v_1),(u_2, v_2)).

Problem 9.3. Consider K_n with vertices $1,\dots,n$ and the weight function where, for $i < j$, we have

$$w(ij) = \begin{cases} j - i & \text{if } j \le i + n/2 \\ i + n - j & \text{if } j > i + n/2 \end{cases}.$$

Convince yourself that placing vertices $1,\dots,n$ evenly on a circle of circumference n, then $w(ij)$ is the arc length distance between i and j. Find an optimal travelling salesman tour on K_n with this weight function.

Solution. We look at K_6 as an example to convince ourselves.



We compute some of the weights.

$$w(12) = 1 \text{ since } 2 \leq 1 + 3 = 4$$
$$w(13) = 2 \text{ since } 3 \leq 1 + 3 = 4$$
$$w(23) = 1 \text{ since } 3 \leq 2 + 3 = 5$$
$$w(26) = 2 \text{ since } 6 > 2 + 3 = 5$$

We see that $w(ij)$ is equal to the arch length in clockwise direction if $j \leq in/2$ and equal to the arch length in counter-clockwise direction if $j > i + n/2$.

Now, we find an optimal travelling salesman tour on K_n with this weight function. We use the circle to visualize the tour and see that the tour with less weight is just going around the circle in either clockwise or counter-clockwise direction. In such a tour we use only one arc (with weight 1) for every new vertex. Any other tour must use more than one arch and therefore give a greater weight.

Problem 9.4. Let $G = (V, E)$ be a connected graph. We use notation as in Theorem 8.27.

(1) Prove that if $C > 0$ is such that $w(k) \geq C$ for every $k \in E$, then
$$w(C_{MST}) \leq 2w(C_{opt}) - 2C.$$
(2) Give an example of a graph G and constant C for which
$$w(C_{MST}) = 2w(C_{opt}) - 2C.$$
(3) (A little harder) Let
$$D = \max_{v \in V} \left(\min_{u \in N(v)} w(uv) \right)$$
and show that we always have
$$w(C_{MST}) \leq 2w(C_{opt}) - 2D.$$

Solution.

(1) We try to mimic the proof of Theorem 8.27 a). Since C_{opt} minus an edge k is a tree, we have that $w(T) \leq w(C_{opt})$ for the tree constructed in phase 1 of MST. Since $w(k) \geq C$, we have that $w(T) + C \leq w(C_{opt})$. Therefore, $w(T_D) \leq 2(w(C_{opt}) - C) = 2w(C_{opt}) - 2C$. The inequality $w(C_{MST}) \leq w(T_D)$ follows from the proof. This gives
$$w(C_{MST}) \leq w(T_D) \leq 2w(C_{opt}) - 2C.$$
(2) First, we explain what the number D is. Let $v \in V$ be given. Then consider $u \in N(v)$ and compute the weights $w(uv)$. Let D_v denote the minimal of these weight, that is, the minimal weight of an edge incident to v. Do this for all $v \in V$ and choose the largest D_v. This is the number D.

We claim that the edge e_D (or one of the edges) corresponding to D, is not in the minimal spanning tree constructed in phase 1 of the minimum spanning tree algorithm. The minimal spanning tree is constructed using the greedy algorithm. We choose an edge of minimal weight (this is not e_d). Then, we choose another edge of minimal weight incident to the first edge. If E_d is incident to the first edge, it will not be minimal, since it is maximal among the minimal. We follow this procedure and observe that we will not choose E_d.

Since we have constructed a spanning tree without E_d, we can use the same approach as in (1) to prove the inequality.

Week of 24 March – Modular arithmetic and finite fields

Warm ups.

(1) Determine the remainders when 3^{15} and 15^{83} are divided by 13.
(2) Is the polynomial $x^2 + x + 1$ irreducible over $\mathbb{Z}_2$? What about over $\mathbb{Z}_3$?
(3) If $f(x)$ is a degree 5 irreducible polynomial over $\mathbb{Z}_p$, how many elements are in the field $\mathbb{Z}_p[x]/\langle f(x)\rangle$?
(4) Show that the polynomial $x^2 + x + 2$ is irreducible over $\mathbb{Z}_3$. What is the product $[x][x^2 + 2]$ in $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$ (i.e. represent the product by a polynomial of degree at most one)? What is the multiplicative inverse of $x + 1$ in $\mathbb{Z}_3[x]/\langle x^2 + x + 2\rangle$?

Solution.

(1) We use that $3^3 \equiv 1 \pmod{13}$. Thus, $3^{15} = (3^3)^5 \equiv 1 \pmod{13}$. Further, we use that $15 = 13 + 2$, and we get that

$$\begin{aligned} 15^{83} &\equiv 2^{83} \pmod{13} \\ &\equiv 2^{4\cdot 20+3} \pmod{13} \\ &\equiv (2^4)^{20} \cdot 2^3 \pmod{13} \\ &\equiv 3^{20} \cdot (-5) \pmod{13} \\ &\equiv (3^3)^6 \cdot 3^2 \cdot (-5) \pmod{13} \\ &\equiv (-4)(-5) \pmod{13} \\ &\equiv 7 \pmod{13} \end{aligned}$$

(2) We check if the polynomial p has any roots in $\mathbb{Z}_2$ and $\mathbb{Z}_3$.

$$\begin{aligned} p(0) &= 0^2 + 0 + 1 \equiv 1 \pmod{2} \\ p(1) &= 1^2 + 1 + 1 = 3 \equiv 1 \pmod{2} \\ p(0) &= 0^2 + 0 + 1 \equiv 1 \pmod{3} \\ p(1) &= 1^2 + 1 + 1 = 3 \equiv 0 \pmod{3} \\ p(2) &= 2^2 + 2 + 1 \equiv 1 + 2 + 1 \pmod{3} \equiv 1 \pmod{3} \end{aligned}$$

We see that $p(1) \equiv 0 \pmod{3}$, thus the polynomial is irreducible over $\mathbb{Z}_3$, but not over $\mathbb{Z}_2$.

(3) The solution to this exercise is described on page 263 in the book. Since the elements in $\mathbb{Z}_p[x]/\langle f(x)\rangle$ are the remainders of division by $f(x)$, that is every element of the form $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ for $a_i \in \mathbb{Z}_5$, there are p^5 elements in $\mathbb{Z}_p[x]/\langle f(x)\rangle$.

(4) We compute the values of the polynomial p over $\mathbb{Z}_3$:

$$\begin{aligned} p(0) &\equiv 2 \pmod{3} \\ p(1) &= 1^1 + 1 + 2 \equiv 1 \pmod{3} \\ p(2) &= 2^2 + 2 + 2 \equiv 1 + 1 \pmod{3} = 2 \pmod{3} \end{aligned}$$

Since $p(i) \not\equiv 0 \pmod 3$, for every $i \in \mathbb{Z}_3$, p is irreducible over $\mathbb{Z}_3$. We have that

$$x(x^2+2) = x^3 + 2x.$$

We find $[x^3+2x]$ in $\mathbb{Z}_3[x]/\langle x^2+x+2\rangle$ by finding the rest after division.

$$\begin{aligned} & x^3 + 2x \qquad : x^2 + x + 2 = x - 1 \\ -&(\underline{x^3 + x^2 + 2x}) \\ & -x^2 \\ -&(\underline{-x^2 - x - 2}) \\ & x + 2 \end{aligned}$$

Thus, $x^3 + 2x = (x-1)(x^2+x+2) + (x+2)$, so $[x^3+2x] = [x+2]$.

The multiplicative inverse of $(x+1)$ in $\mathbb{Z}_3[x]/\langle x^2+x+2\rangle$ is a linear polynomial $ax+b$ such that that

$$(x+1)(ax+b) \equiv 1 \pmod{x^2+x+2}.$$

We must find a $K \in \mathbb{Z}_3, k \not\equiv 0$ such that

$$(x+1)(ax+b) - 1 = ax^2 + (a+b)x + b - 1 = K(x^2+x+2)$$

Thus,

$$\begin{aligned} a &= K \\ (a+b) &= K \\ b - 1 &= 2K \end{aligned}$$

If $K = 1$, then $b - 1 = 2K$ does not have a solution in $\mathbb{Z}_3$. If $K = 2$, we get $b = 0$. Thus, $2x$ is the inverse of $(x+1)$ in $\mathbb{Z}_3[x]/\langle x^2+x+2\rangle$.

Problem 10.1. Solve the set of equations

$$\begin{aligned} x + 2y &= 4 \\ 4x + 3y &= 4 \end{aligned}$$

in $\mathbb{Z}_7$ and $\mathbb{Z}_5$. It will be useful to first know the multiplicative inverses of 2 and 3 in both fields.

Solution. We follow the hint and find the multiplicative inverses of 2 and 3 in both fields.

$$\begin{aligned} 2 \cdot 4 = 8 \equiv 1 \pmod 7 \\ 3 \cdot 5 = 15 \equiv 1 \pmod 7 \end{aligned}$$

$$2 \cdot 3 = 6 \equiv 1 \pmod 5,$$

thus 4 is the inverse of 2 and 5 the inverse of 3 in $\mathbb{Z}_7$, and 2 and 3 are inverses in $\mathbb{Z}_5$.

We solve the set of equations in $\mathbb{Z}_7$. We put $x = 4 - 2y$ into the second equation and get

$$\begin{aligned} 4(4-2y) + 3y - 4 \equiv 0 \pmod 7 \\ 5y \equiv 5 \pmod 7 \end{aligned}$$

$$y \equiv 3 \cdot 5 \pmod 7$$
$$y \equiv 1 \pmod 7$$

Further, we have $x \equiv 4 - 2 \cdot 1 \pmod 7 \equiv 2 \mod 7$.

We solve the set of equations in $\mathbb{Z}_5$ by multiplying the first equation by 3 and the second equation by 2. We get

$$3x + y \equiv 2 \pmod 5$$
$$3x + y \equiv 3 \pmod 5$$

We see that this set of equations has no solution.

Problem 10.2. Let p be a prime number.

(1) Prove that for $1 \leq i \leq p-1$, we have
$$\binom{p}{i} \equiv 0 \pmod p$$

(2) Use the binomial theorem to prove that for all , $b \in \mathbb{Z}$, we have

(C)
$$(a+b)^p \equiv a^p + b^p \pmod p.$$

(3) One form of Fermat's little theorem says that for all $a \in \mathbb{Z}$, we have $a^p \equiv a \pmod p$. Give a proof of this statement using induction and Equation (C).

Solution.

(1)
$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{i!(p-i)!} \equiv 0 \pmod p$$
Since p is prime and $1 \leq i \leq p-1$, non of the factors in $i!(p-i)!$ will divide p.

(2)
$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \equiv \binom{p}{0} a^0 b^p + \binom{p}{p} a^p b^{p-p} \pmod p.$$
Thus,
$$(a+b)^p \equiv a^p + b^p \pmod p.$$

(3) The theorem holds for $a = 0$, indeed $0^p \equiv 0 \pmod p$. Assume $a \geq 0$ and that $a^p \equiv a \pmod p$. We want to prove that $(a+1)^p \equiv a+1 \pmod p$.
$$\begin{aligned}(a+1)^p &\equiv a^p + 1^p \pmod p \\ &\equiv a^p + 1 \pmod p \\ &\equiv a + 1 \pmod p,\end{aligned}$$
where we used the induction hypothesis in the last step.

Assume now that $a \leq 0$ and that $a^p \equiv a \pmod p$. Then
$$\begin{aligned}(a-1)^p &\equiv a^p + (-1)^p \pmod p \\ &\equiv a^p - 1 \pmod p \\ &\equiv a - 1 \pmod p,\end{aligned}$$
and the theorem is proven. Observe that this also holds for $p = 2$. Indeed, $(-1)^2 \equiv -1 \pmod 2$, since $-1 = (-1) \cdot 2 + 1$.

Problem 10.3. Decompose $x^4 + 1 \in \mathbb{Z}_3[x]$ into irreducible factors.

Solution. First, we check if $p(x) = x^4+1$ has a root in $\mathbb{Z}_3$. We see that $p(0), p(1), p(2) \not\equiv 0 \pmod 3$. Thus, $p(x)$ does not have any root in $\mathbb{Z}_3$, so there are no linear factors in the decomposition. Thus, we have to find polynomials $a_0 + a_1x + a_2x^2$ and $b_0 + b_1x + b_2x^2$ such that

$$(a_0 + a_1x + x^2)(b_0 + b_1x + x^2) = x^4 + 1$$

We write out the equation.

$$a_0 + b_0 + (a_0b_1 + a_1b_0)x + (a_0 + a_1b_1 + b_0)x^2 + (a_1 + b_1)x^3 + x^4 = x^4 + 1$$

Thus

$$\begin{aligned} a_0 + b_0 &= 1 \\ a_0b_1 + a_1b_0 &= 0 \\ a_0 + a_1b_1 + b_0 &= 0 \\ a_1 + b_1 &= 0 \end{aligned}$$

We use $a_1 = -b_1$ and $a_0 + b_0 = 1$ and get

$$\begin{aligned} a_0 + b_0 &= 1 \\ a_0b_1 + (-b_1)b_0 = b_1(a_0 - b_0) &= 0 \\ (-b_1)b_1 + 1 &= 0 \\ a_1 + b_1 &= 0 \end{aligned}$$

The two last equations are fulfilled only if $a_1 = 1, b_1 = 2$ (or the opposite). The two first equations are fulfilled if $a_0 = b_0 = 2$. This gives the decomposition

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

Problem 10.4. Let $p > 2$ be a prime. We say an element a of a field F is a square if there is some $b \in F$ such that $b^2 = a$.

(1) Prove that for $a, b \in \mathbb{Z}_p$, we have $a^2 = b^2$ if and only if $a = b$ og $a = -b$.
(2) Prove that the set of squares in $\mathbb{Z}_p$ has $(p - 1)/2$ elements.
(3) Prove that the polynomial $x^2 - a \in \mathbb{Z}_p[x]$ is irreducible if and only if a is not a square in Z_p.
(4) Prove that for $a \in \mathbb{Z}_p \setminus \{0\}$, we have $a = a^{-1}$ if and only if $a = 1$ or $a = p - 1$.
(5) Use the previous point to prove **Wilson's theorem**:
$$(p - 1)! \equiv -1 \pmod p.$$
Hint: Show that all factors $2, 3 \ldots, p-2$ cancel out pairwise in the field $\mathbb{Z}_p$.
(6) Let $n \geq 1$. Prove that if $a, b \in GF(2^n)$ are such that $a^2 = b^2$, then $a = b$.
(7) Prove that every element in $GF(2^n)$ is a square.

Solution.

(1) The first direction is clear. For the other direction, assume $a, b \in \mathbb{Z}_p$ such that $a^2 = b^2$. Thus,
$$a^2 - b^2 = (a - b)(a + b) \equiv 0 \pmod p$$
Since p is prime, this holds only if $a - b \equiv 0 \pmod p$ or $a + b \equiv 0 \pmod p$, thus either $a \equiv b \pmod p$ or $a \equiv -b \pmod p$.

(2) We use the previous exercise. Since $a^2 = b^2$ if and only if $a = b$ or $a = -b$, every square can be obtained by taking the square of two different (but inverse) elements. If two elements are not inverses, we get different squares. Thus, we get $\frac{p-1}{2}$ squares (we subtract 1 since we have assumed $a \neq 0$).

(3) Assume $p(x) = x^2 - a \in \mathbb{Z}_p[x]$ is irreducible. Since the polynomial has degree 2, this means that p has no roots in $\mathbb{Z}_p[x]$. Thus, there does not exists a $b \in \mathbb{Z}_p$ such that $b^2 = a$. This is the same as saying that a is not a square in $\mathbb{Z}_p$.

For the other direction, assume that a is not a square. Thus, there does not exists a $b \in \mathbb{Z}_p$ such that $b^2 = a$. This shows that $x^2 - a$ cannot have a root in $\mathbb{Z}_p$, thus p is irreducible in $\mathbb{Z}_p[x]$.

(4) Recall that a^{-1} is an element such that $a \cdot a^{-1} = 1$. If $a = 1$, then $1 \cdot 1 = 1$, thus $a = a^{-1}$. If $a = p-1$, then $(p-1) \cdot (p-1) = p^2 + 1 \equiv 1 \pmod{p}$, thus $a = a^{-1}$.

For the other direction, assume $a = a^{-1}$. We multiply by a on both sides, and get that $a^2 - 1 \equiv 0 \pmod{p}$. Thus, $a^2 \equiv 1 \pmod{p}$. We have that $a = 1$ or $a = -1$ (by (1)). In $\mathbb{Z}_p$ we have that $p - 1 \equiv -1 \pmod{p}$.

(5) We follow the hint and show that all factors $2, 3 \ldots, p-2$ cancel out pairwise in the field $\mathbb{Z}_p$. That is, we will argue that the factors are pairwise inverses of each other and that we therefore get that $2 \cdot 3 \ldots (p-2) \equiv 1^{(p-3)/2} \pmod{p} \equiv 1 \pmod{p}$. Indeed, from (4), we have that $a = a^{-1}$ iff $a = 1$ or $a = p - 1$. Thus, for $a \in \{2, 3, \ldots, p-2\}$, $a \neq a^{-1}$. Since inverses are unique modulo, the elements are pairwise inverses of each other. This gives

$$\begin{aligned}(p-1)! = 2 \cdot 3 \ldots (p-2) \cdot (p-1) &\equiv 1 \cdot (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}.\end{aligned}$$

(6) First, we prove that for every $a \in GF(2^n)$, $a = -a$. Indeed, as we saw in Warm ups (3), the field $\mathbb{Z}_p[x]/\langle f(x)\rangle$ consists of p^n elements, where n is the degree of $f(x)$. Since there exists precisely one finite field $GF(q)$ for each $q = p^n$ up to isomorphism. Thus, $G(2^n)$ is isomorphic to $Z_2[x]/\langle f(x)\rangle$ for an f of degree n. The elements in $Z_2[x]/\langle f(x)\rangle$ are on the form $a_0 + a_1 x$ for $a_i \in Z_2$. We have that $a_i = -a_i$ for $a_i \in \mathbb{Z}_2$. This gives that

$$a_0 + a_1 x = -a_0 - a_1 x = -(a_0 + a_x),$$

thus $a = -a$ for $a \in GF(2^n)$. Assume now that $a^2 = b^2$. Thus,

$$a^2 - b^2 = (a + b)(a - b) = 0.$$

This gives that either $a = b$ or $a = -b$, but since $b = -b$, we have that $a = b$.

(7) By the previous result, squaring each of the 2^n elements in $GF(2^n)$ gives 2^n different squares, every element in 2^n must be a square (by the pigeonhole principle.)

Week of 31 March – Latin squares and designs

Warm ups.

(1) How many mutually orthogonal Latin squares are there of order 5? Find a pair of them.

(2) Why is there at least one pair of orthogonal Latin squares of order 12?

(3) Write down the blocks $B_1, \ldots, B_7 \subset \{1, \ldots, 7\}$ for the 2-design from the Fano plane.
(4) How many lines and points are in a finite projective plane of order 3? How many points are on each line?

Solution.

(1) See pages 266-277 in the book.
(2) This follows from Corollary 12.5 on page 268 in the book. Since $12 \equiv 0 \pmod 4$, $N(12) \geq 2$.
(3)

$$B_1 = \{1, 2, 4\}$$
$$B_2 = \{1, 5, 6\}$$
$$B_3 = \{1, 3, 7\}$$
$$B_4 = \{2, 6, 7\}$$
$$B_5 = \{2, 3, 5\}$$
$$B_6 = \{3, 4, 6\}$$
$$B_7 = \{4, 5, 7\}$$

(4) From Theorem 12.11, we get that there are n^2+n+1 vertices and $k = n+1$ vertices on each edge, where n is the order of the projective plane. For $n = 3$, we get $3^2 + 3 + 1 = 13$ vertices and $3 + 1 = 4$ vertices on each edge.

Problem 11.1. Let $L_1, L_2 : \{1, \ldots, n\} \times \{1, \ldots, n\} \to \{1, \ldots, n\}$ be orthogonal Latin squares, and let π be a permutation of $\{1, \ldots, n\}$.

(1) Let $L_1'(i, j) = L_1(\pi(i), j)$ and $L_2'(i, j) = L_2(\pi(i), j)$. Show that L_1' and L_2' are Latin squares and that they are orthogonal to one another.
(2) Let $L_2''(i, j) = \pi(L_2(i, j))$. Show that L_2'' is a Latin square and that L_1 and L_2'' are orthogonal to one another.

Solution.

(1) Let $k = \{1, 2\}$. We have to show that if $L_k'(i, j) = L_k'(i', j)$, then $i = i'$ and if $L_k'(i, j) = L_k'(i, j')$, then $j' = j$. Assume $L_k'(i, j) = L_k'(i', j)$. Thus,

$$L_k(\pi(i), j) = L_k(\pi(i'), j).$$

Since L_k are Latin squares, $\pi(i) = \pi(i')$. Since π is a permutation, $i = i'$. Assume $L_k'(i, j) = L_k'(i, j')$. Thus,

$$L_k(\pi(i), j) = L_k(\pi(i), j').$$

Since L_k are Latin squares, $j = j'$.

Now, we show that L_1' and L_2' are orthogonal to one another. Let $(a_1, a_2) \in \{1, \ldots, n\}$. Assume that we have two pairs (i, j) and (i', j') such that

$$L_1'(i, j) = L_1(\pi(i), j) = a_1 \quad L_2'(i, j) = L_2(\pi(i), j) = a_2$$
$$L_1'(i', j') = L_1(\pi(i'), j') = a_1 \quad L_2'(i', j') = L_2(\pi(i'), j') = a_2$$

Since L_1 and L_2 are orthogonal, we have that $\pi(i) = \pi(i')$ and $j = j'$. Thus, $i = i'$ and $j = j'$, so L_1' and L_2' are also orthogonal to one another.

(2) Assume $L_2''(i,j) = L_2''(i',j)$. Thus,

$$\pi(L_2(i,j)) = \pi(L_2(i',j))$$

Since π is a permutation, we have that $L_2(i,j) = L_2(i',j)$, and since L_2 is a Latin square, $i = i'$. The same holds for the analogues case.

Now, we show that L_2'' and L_1 are orthogonal to one another. Let $(a_1, a_2) \in \{1, \dots, n\}$. Assume that we have two pairs (i,j) and (i',j') such that

$$\begin{aligned} L_1(i,j) = a_1 \quad L_2''(i,j) = \pi(L_2(i,j)) = a_2 \\ L_1(i',j') = a_1 \quad L_2''(i',j') = \pi(L_2(i',j') = a_2 \end{aligned}$$

Since π is a permutation, $L_2(i,j) = L_2(i',j') = b$. Since L_1 and L_2 are orthogonal, $i = i'$ and $j = j'$ (we use the definition of orthogonality on the pair (a_1, b)). Thus, L_1 and L_2'' are orthogonal.

Problem 11.2. Construct a pair of orthogonal Latin squares of order 12.

Solution. We follow the construction given in the proof of Theorem 12.4 in the book. First, we find two orthogonal Latin squares L_1, L_2 of order 3 and two orthogonal Latin squares L_1', L_2' of order 4 by following the algorithm described on page 266. We have for example:

$$L_1 = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 0 & 1 \\ \hline \end{array} \qquad L_2 = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 2 & 0 & 1 \\ \hline 1 & 2 & 0 \\ \hline \end{array}$$

$$L_1' = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array} \qquad L_2' = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline \end{array}$$

We set $A = \{0, 1, 2\}$ and $B = \{0, 1, 2, 3\}$ and $C = A \times B$. This means that an element $c \in C$ is on the form (a, b), where $a \in A$ and $B \in B$. Thus,

$$\begin{aligned} C = \{&(0,0), (0,1), (0,2), (0,3), \\ &(1,0), (1,1), (1,2), (1,3), \\ &(2,0), (2,1), (2,2), (2,3)\} \end{aligned}$$

We see that C has 12 elements. We will use these elements instead of the numbers $\{0, \dots, 11\}$. The orthogonal Latin squares of order 12 will be L_1^* and L_2^*, where

$$L_h^*((i,i'),(j,j')) = (L_h(i,j), L_h'(i',j')),$$

where $i, j \in A$ and $i', j' \in B$. First, we find the first row of L_1^*.

$$L_1^*((0,0),(0,0)) = (L_1(0,0), L_1'(0,0)) = (0,0)$$
$$L_1^*((0,0),(0,1)) = (L_1(0,0), L_1'(0,1)) = (0,1)$$
$$L_1^*((0,0),(0,2)) = (L_1(0,0), L_1'(0,2)) = (0,2)$$
$$L_1^*((0,0),(0,3)) = (L_1(0,0), L_1'(0,3)) = (0,3)$$
$$L_1^*((0,0),(1,0)) = (L_1(0,1), L_1'(0,0)) = (1,0)$$
$$L_1^*((0,0),(1,1)) = (L_1(0,1), L_1'(0,1)) = (1,1)$$
$$L_1^*((0,0),(1,2)) = (L_1(0,1), L_1'(0,2)) = (1,2)$$
$$L_1^*((0,0),(1,3)) = (L_1(0,1), L_1'(0,3)) = (1,3)$$
$$L_1^*((0,0),(2,0)) = (L_1(0,2), L_1'(0,0)) = (2,0)$$
$$L_1^*((0,0),(2,1)) = (L_1(0,2), L_1'(0,1)) = (2,1)$$
$$L_1^*((0,0),(2,2)) = (L_1(0,2), L_1'(0,2)) = (2,2)$$
$$L_1^*((0,0),(2,3)) = (L_1(0,2), L_1'(0,3)) = (2,3)$$

We have found the first (the $(0,0)$th) row of the first Latin square of order 12:

$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-

We compute the next row:

$$L_1^*((0,1),(0,0)) = (L_1(0,0), L_1'(1,0)) = (0,1)$$
$$L_1^*((0,1),(0,1)) = (L_1(0,0), L_1'(1,1)) = (0,0)$$
$$L_1^*((0,1),(0,2)) = (L_1(0,0), L_1'(1,2)) = (0,3)$$
$$L_1^*((0,1),(0,3)) = (L_1(0,0), L_1'(1,3)) = (0,2)$$
$$L_1^*((0,1),(1,0)) = (L_1(0,1), L_1'(1,0)) = (1,1)$$
$$L_1^*((0,1),(1,1)) = (L_1(0,1), L_1'(1,1)) = (1,0)$$
$$L_1^*((0,1),(1,2)) = (L_1(0,1), L_1'(1,2)) = (1,3)$$
$$L_1^*((0,1),(1,3)) = (L_1(0,1), L_1'(1,3)) = (1,2)$$
$$L_1^*((0,1),(2,0)) = (L_1(0,2), L_1'(1,0)) = (2,1)$$
$$L_1^*((0,1),(2,1)) = (L_1(0,2), L_1'(1,1)) = (2,0)$$
$$L_1^*((0,1),(2,2)) = (L_1(0,2), L_1'(1,2)) = (2,3)$$

$$L_1^*((0,1),(2,3)) = (L_1(0,2), L_1'(1,3)) = (2,2)$$

$(0,0)$	$(0,1)$	$(0,2)$	$(0,3)$	$(1,0)$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$
$(0,1)$	$(0,0)$	$(0,3)$	$(0,2)$	$(1,1)$	$(1,0)$	$(1,3)$	$(1,2)$	$(2,1)$	$(2,0)$	$(2,3)$	$(2,2)$
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-	-	-	-

We continue in this way for the remaining rows, and for the Latin square L_2^*.

Problem 11.3. Let $G = (V, E)$ be a graph. Show that E are the blocks of a 1-design on V with $(v, k, \lambda) = (|V|, 2, \lambda)$ if and only if G is λ-regular.

Solution. Let $G = (V, E)$ be a graph and assume that E are the blocks of a 1-design on V with $(v, k, \lambda) = (|V|, 2, \lambda)$. This means that for every block $e \in E$, there are 2 elements from V, that is there are 2 vertices for every edge. Further, every 1-set, that is every vertex, is contained in exactly λ sets from E, that is λ edges. This is the definition of a λ-regular graph.

For the other direction. Assume that $G = (V, E)$ is a λ-regular graph. Use the definition of a λ-regular graph to explain that E are the blocks of a 1-desgin on V with $(v, k, \lambda) = (|V|, 2, \lambda)$

Problem 11.4. Consider the set of squares on a chessboard $S = \{1, \ldots, 8\} \times \{1, \ldots, 8\}$. Say that squares are *related* if they lie in the same row or the same column. Is there a permutation $\pi : S \to S$ with the property that for every pair of related squares s_1, s_2, we have that $\pi(s_1)$ and $\pi(s_2)$ are not related? *Hint: Write* $\pi(i,j) = (\pi_1(i,j), \pi_2(i,j))$. *What can you say about* π_1 *and* π_2*?*

Solution. We write the conditions on π in terms of π_1 and π_2. A point (i, j) is related to (i, k) and (k, j) for $k \in \{1, \ldots, 8\}$. Thus, we must have that

$$\begin{aligned}
\pi_1(i,j) &\neq \pi_1(i,k) \text{ for } k \neq j \\
\pi_1(i,j) &\neq \pi_1(k,j), \text{ for } k \neq i \\
\pi_2(i,j) &\neq \pi_2(i,k), \text{ for } k \neq j \\
\pi_2(i,j) &\neq \pi_2(k,j), \text{ for } k \neq i
\end{aligned}$$

Thus, π_1 and π_2 must be Latin squares. Since π is a permutation, we also get that for $(a_1, a_2) \in S$, if $\pi(i,j) = (a_1, a_2)$ and $\pi(i', j') = (a_1, a_2)$, then $i = i'$ and $j = j'$. This condition means that π_1 and π_2 must be orthogonal. We have reformulated the problem to the following: *Does there exists two mutually orthogonal Latin squares of order 8.* The answer is yes (see the book), so there exists a $\pi : S \to S$ with the

property that for every pair of related squares s_1, s_2, we have that $\pi(s_1)$ and $\pi(s_2)$ are not related.

Problem 11.5. Let $D(v,k,\lambda)$ be a 2-design with b blocks $B_1,\dots,B_b$ on $\{1,...,v\}$ and $M=(m_{ij})$ the $v\times b$ matrix given by $m_{ij}=1$ if $i\in B_j$ and $m_{ij}=0$ if $i\notin B_j$. The goal of this problem is to show that if $k<v$, then $v\leq b$.

Let $A=MM^T$.

(1) Show that $A_{ij}=\lambda$ for $i\neq j$.
(2) Show that $A_{ii}=\lambda(v-1)/(k-1)$.
(3) Let $\overrightarrow{x},\overrightarrow{y}\in\mathbb{R}^v$ be such that $\overrightarrow{y}=A\overrightarrow{x}$. Let $x=\sum_{i=1}^v x_i$. Prove that $y_i=\lambda(x+\frac{v-k}{k-1}x_i)$ for all i.
(4) Prove that if $k<v$, then $\overrightarrow{y}=0\Leftrightarrow\overrightarrow{x}=0$.
(5) Assume $k<v$. Justify each the (in-)equalities
$$v=\mathrm{rk}(A)\leq\mathrm{rk}(M)\leq b$$
to conclude that $v\leq b$.

Solution.

(1) Let $i\neq j$. Then $A_{ij}=\sum_{l=1}^b m_{il}\cdot m_{jl}$. The product $m_{il}\cdot m_{jl}$ is 1 if $i\in B_l$ and $j\in B_l$ and zero if either $i\notin B_l$ or $j\notin B_l$. Since D is a 2-design the pair (i,j) is in λ blocks. Thus, there are λ ls such that $m_{il}\cdot m_{jl}=1$, so $A_{ij}=\sum_{l=1}^b m_{il}\cdot m_{jl}=\lambda$.
(2) We have that $A_{ii}=\sum_{l=1}^b m_{il}^2$. Thus, A_{ii} is equal to the number of times m_{il} is equal to 1, which is the number of blocks B_l such that $i\in B_l$. For every pair (i,i') for $1\leq i'\leq v$, $i\neq i'$, there are λ blocks B_l such that $(i,i')\in B_l$, which gives $\lambda(v-1)$ blocks. But since there are $k-1$ other elements than i in each B_l, we have to divide by $k-1$. Thus, the number of blocks B_l such that $i\in B_l$ is $\lambda(v-1)/(k-1)$.
(3)
$$\begin{aligned}y_i=\sum_{j=1}^v A_{ij}x_j&=\lambda\frac{v-1}{k-1}x_i+\sum_{j=1,j\neq i}^v\lambda x_j\\&=\lambda(\frac{v-1}{k-1}x_i+(-x_i)+x)\\&=\lambda(\frac{v-k}{k-1}x_i+x).\end{aligned}$$
(4) Let $k<v$. Assume $\overrightarrow{x}=0$, thus $\sum_{i=1}^v x_i=\sum_{i_1}^v 0=0$. Thus, $y_i=\lambda(\frac{v-k}{k-1}0+0)=0$, and $\overrightarrow{y}=0$.

Assume $\overrightarrow{y}=0$. Thus, $y_i=0$ for every i. Thus,
$$\begin{aligned}\lambda(\frac{v-k}{k-1}x_i+x)&=0\\\frac{v-k}{k-1}x_i+x&=0\\\frac{v-k}{k-1}x_i&=-x\\x_i&=-\frac{k-1}{v-k}x\end{aligned}$$

Since $k < v$, the fraction ha positive sign, thus x_i is equal to a negative fraction of x for every i. This holds only if each $x_i = 0$. Thus, $\overrightarrow{x} = 0$.

(5) Let $k < v$. First, we prove that $v = \mathrm{rk}(A)$. Since $\overrightarrow{y} = 0$ if and only if $\overrightarrow{x} = 0$, $\ker(A) = 0$ and thus, $\mathrm{rk}(A) = \dim A = v$.

Further, we prove that $\mathrm{rk}(A) \leq \mathrm{rk}(M)$. We use that if A is an $n \times k$-matrix and B a $k \times n$-matrix, $\mathrm{rk}(AB) \leq \min(\mathrm{rk}(A), \mathrm{rk}(B))$. Thus,

$$\mathrm{rk}(A) = \mathrm{rk}(MM^T) \leq \mathrm{rk}(M),$$

since $\mathrm{rk}(M) = \mathrm{rk}(M^T)$.

The last inequality follows since M is a $v \times b$-matrix and thus, $\mathrm{rk}(M) \leq b$.

Week of 7 April – Finite projective planes

Problem 12.1. Let

$$S = \{s_1, \dots s_v\}$$

and let

$$\mathcal{B} = \{B_1 \dots, B_b\}$$

where the B_i are distinct subsets of S. The **incidence matrix** of $(S, \mathcal{B})$ is the $(v \times b)$-matrix M such that

$$m_{jk} = \begin{cases} 1 \text{ if } s_j \in B_k \\ 0 \text{ if } s_j \notin B_k \end{cases}$$

(1) Write down the 7×7 incidence matrix for the Fano plane.

(2) Let $(S, \mathcal{B})$ be a finite projective plane of order n, with incidence matrix M.

(a) Show that dot product of two distinct column vectors of M is 1, and that the dot product of two distinct row vectors of M is 1.

(b) Show that

$$M^T M = MM^T = nI + A,$$

where I is the identity matrix and A is the matrix with entries only ones.

Solution.

(1) We let

$$\begin{aligned} &B_1 = \{1, 2, 4\}, \quad B_2 = \{1, 5, 6\}, \quad B_3 = \{1, 3, 7\}, \\ &B_4 = \{2, 6, 7\}, \quad B_5 = \{2, 3, 5\}, \quad B_6 = \{3, 4, 6\}, \\ &B_7 = \{4, 5, 7\} \end{aligned}$$

Thus,

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(2) (a) Let R_u and R_v be two distinct rows in M. Then $R_u \cdot R_v = \sum_{i=1}^{v} m_{ui}m_{vi}$. The product $m_{ui}m_{wi}$ is 1 if and only if $s_u, s_w \in B_i$. In a projective plane, each 2-subset is contained in exactly 1 set from $\mathcal{B}$ (pkt (i) in Definition 12.10), thus there exists one i such that $m_{ui}m_{wi} = 1$. Otherwise, $m_{ui}m_{wi} = 0$.
Let now C_u and C_w be two distinct columns in M. Then $C_u\dot{C}_w = \sum_{i=1}^{k} m_{iu}m_{iw}$. The product $m_{iu}m_{iw}$ is 1 if and only if $s_i \in B_u, B_w$. By pkt. (ii) in Definition there exists only one i such that $s_i \in B_u, B_w$. Thus, $C_u \cdot C_w = \sum_{i=1}^{k} m_{iu}m_{iw}$.

(b) Let $B = M^T M$ and let $i \neq j$. We have that b_{ij} is the dot product of the ith and jth columns i M. Thus $b_{ij} = 1$. Further, $b_{ii} = \sum_{l=1}^{v} m_{li}^2$. Since there are $n+1$ points on each line in a profjective plane of order n, there are n ls such that $m_{li}^2 = 1$. Thus $b_{ii} = \sum_{l=1}^{v} m_{li}^2 = n+1$. We therefore get that B is a matrix with $n+1$ on the diagonal and 1 elsewhere and we see that B can be decomposed a $nI + A$. The same argument holds for MM^T.

Problem 12.2. Let $(S, \mathcal{B})$ be a finite projective plane of order n, i.e. where S is the set of points and $\mathcal{B} \subseteq 2^S$ is the set of lines. We construct a new pair $(S', \mathcal{B}')$ as follows. Let $S' = \mathcal{B}$. For every $x \in S$, define $l_x \subseteq S'$ by

$$l_x = \{l \in \mathcal{B} \mid x \in l\},$$

and let $\mathcal{B}'$ be the set of all l_x. Prove that $(S', \mathcal{B}')$ is a projective plane.

Solution. We prove that $(S', \mathcal{B}')$ satisfies the definition of a projective plane (Definition 12.10).

(i) Let $u \neq v \in S'$. We need to prove that there exists precisely one line $l_x \in \mathcal{B}'$ such that $\{u, v\} \in l_x$. Thus, we must have $x \in S$ such that $x \in u, v$. Since $u, v \in S' = \mathcal{B}$ and $(S, \mathcal{B})$ is a projective plane, we know that there exists only one $s \in S$ such that $s \in u \cap v$. Thus, there exists only one l_x such that $u, v \in l_x$.

(ii) Let $l_x \neq l_y \in \mathcal{B}'$. We need to prove that there exists exactly one point $u \in S'$ such that $u \in l_x \cap l_y$. Such an u is satisfies that $x \in u$ and $y \in u$ for $x, y \in S$. Since $(S, \mathcal{B})$ is a projective plane, there exists only one such u.

(iii) Follow the same procedure as in (i) and (ii).

Problem 12.3. Let $(S, \mathcal{B})$ be the projective plane of order 5 constructed from the field of five elements $\mathbb{Z}_5$. For a vector $(x, y, z) \in \mathbb{Z}_5^3 \setminus \{\overrightarrow{0}\}$, we let $[x : y : z] \in S$ be the subspace spanned by (x, y, z), that is

$$[x : y : z] = \mathbb{Z}_5(x, y, z) = \{(\alpha x, \alpha y, \alpha z) \mid \alpha \in \mathbb{Z}_5\}.$$

(1) How many points are contained in a line in the projective plane?
(2) Let l be the line containing points $[2 : 3 : 1]$ and $[1 : 2 : 3]$. List the points of l in the form $[x : y : z]$.
(3) Let $W = \{(x, y, z) \in \mathbb{Z}_5^3 \mid x+y+z = 0\} \subseteq \mathbb{Z}_5^3$, and let l' be the corresponding line in the projective plane. List the points l' in the forms $[x : y : z]$.
(4) Find $l \cap l'$.

Solution.

(1) In the projective space of order 5, $5+1=6$ points are contained in a line.
(2) The other 4 points on the line containing $[2:3:1]$ and $[1:2:3]$ are

$$\begin{aligned}[2:3:1]+[1:2:3]&=[3:0:4]\\ [2:3:1]+2[1:2:3]&=[4:2:2]=[2:1:1]\\ [2:3:1]+3[1:2:3]&=[0:4:0]=[0:1:0]\\ [2:3:1]+4[1:2:3]&=[1:1:3]\end{aligned}$$

(3) We have that $[1:2:2]\in l'$ and $[0:1:4]\in l'$. Thus, the other 4 are

$$\begin{aligned}[1:2:2]+[0:1:4]&=[1:3:1]\\ [1:2:2]+2[0:1:4]&=[1:4:0]\\ [1:2:2]+3[0:1:4]&=[1:0:4]\\ [1:2:2]+4[0:1:4]&=[1:1:3]\end{aligned}$$

(4) We see that $[1:1:3]$ is a point of both l and l'.

Problem 12.4. (Inspired by the card game SET). Let $n\geq 1$, and let $S=\mathbb{Z}_3^n$. Define a SET in S to be a $B=\{v_1,v_2,v_3\}\subseteq S$ with the v_i all distinct, such that $v_1+v_2+v_3=0$. Let $\mathcal{B}_n$ be the set of all SETs.

(1) Prove that $(S,\mathcal{B})$ forms a Steiner system, and determine $|\mathcal{B}|$.
(2) A **cap set** is a subset $T\subseteq S$, such that T contains no SET. Find the maximal possible size of a cap set when $n=1$ and when $n=2$.

Solution.

(1) We have to prove that $(S,\mathcal{B})$ a Steiner system $S_t(v,k)$, where $v=|S|=3^n$ and $k=|B|=3$. We have to prove that each 2-subset is contained in exactly one set from $\mathcal{B}$. This means that given v_1,v_2, v_3 is uniquely defined. Since $v_1+v_2+v_3=0$, $v_3=-(v_1+v_2)$.

The size of $\mathcal{B}$ is the number of ways to make unordered 3-tuples (v_1,v_2,v_3). Since v_3 is determined by v_1 and v_2, we only need to choose them, thus $3^n\cdot(3^n-1)$ possibilities. Since the 3-tuple is unordered, we divide by $3!=6$. Thus,

$$|\mathcal{B}|=\frac{1}{6}(3^n\cdot(3^n-1)).$$

(2)

- When $n=1$, $S=\{0,1,2\}$, thus the cap sets are the subset with two elements. The maximal possible size of a cap set is therefore 2.
- When $n=2$, $S=\{(0,0),(0,1),(1,0)(1,1),(2,0),(0,2),(2,2),(2,1),(1,2)\}$. An example of a cap set is $T=\{(0,0),(0,1),(1,0)(1,1)\}$. We claim that the maximal possible size of a cap set is four. Indeed, since T is a cap set for $x,y\in T$, $-(x+y)\notin T$. There are $\binom{4}{2}=6$ ways to choose x,y and there 5 elements in $S\setminus T$. We claim that there exists

only 1 $z \in S \setminus T$ such that $-(x+y) = z$ and $-(x'+y') = z$ where $x \neq y \neq x' \neq y' \in T$. Assume for contradiction that

$$x + y = -z$$
$$x' + y' = -z$$

and

$$x + x' = -z'$$
$$y + y' = -z'$$

Thus,

$$x + y + x' + y' = -2z = -2z',$$

so $z = z'$. Thus,

$$x + y = -z$$
$$x + x' = -z$$

which implies that $x + z = -y = -x'$. But we assumed that $y \neq x'$, so we have a contradiction.

Problem 12.5. Let $A = \{0, 1\}$.

(1) Determine which of the codes $C = \{0, 10, 11\}$, $D = \{1, 10, 11\}$ and $E = \{0, 01, 11\}$ are prefix codes.
(2) Let $X = \{\alpha, \beta, \gamma\}$, and suppose we encode messages written in the alphabet X using the above codes. Determine for which of the alphabets C, D and E a message can always be decoded uniquely.

Solution.

(1) C is a prefix code since 10 and 11 does not have 0 as prefix. D is not a prefix code since 10 and 11 as 1, another word in the code, as prefix. E is not a prefix code since 01 has 0, another word in the code, as prefix.
(2) A prefix code can always be decoded uniquely, thus C can be decoded uniquely. The code E can also be decoded uniquely if the encoding is done backwards, since the code is a "backward prefix code".

Problem 12.6. Let $A = \{0, 1\}$ and let $C \subseteq A^*$ be a code. The **length sequence** of C is the lengths of the code words in C listed in ascending order, i.e. the code $\{0, 1, 100, 0100\}$ has length sequence $1, 1, 3, 4$.

(1) Prove that there is no prefix code C with length sequence

$$1, 2, 2, 2.$$

(2) Prove that for $n \geq 3$, there is no prefix code C with length sequence

$$1, 2, \ldots, n-1, n, n, n.$$

Solution.

(1) There are fours words of length 2 in the alphabet $\{0,1\}$, $00, 01, 10, 11$. Since the length sequence of C has first element 1, the first word in the code is either 0 or 1. Assume the word is 0 Then, the words of length 2 cannot start with 0, so there are two remaining words. This shows that the length sequence cannot be 1,2,2,2.
(2) The same argument holds in this case. For each n, there are only two possibilities that don't have any of the words as prefix. Thus, the length sequence cannot be $1, 2, \ldots, n-1, n, n, n$.

Week of 21 April – Hamming distance and error correcting codes

Warm-ups.

(1) What is the Hamming distance between 0010 and 0100?
(2) What is the maximal Hamming distance between two code words in $\{0,1\}^n$?
(3) For which t is the code $\{0000, 0011, 1100\}$ t-error detecting? For which t is it t-error correcting?
(4) What is the Hamming bound for the size of a code $C \subseteq \{0,1,2\}^4$ with $d(C) \geq 3$?

Solution.

(1) $\Delta(0010, 0100) = 2$.
(2) The maximal Hamming distance between two code words in $\{0,1\}^n$ is n, that is when every letter is different in the two codes.
(3) A code C is t-error detecting if for all $x \in C$, $B_t(x) \cap C = \{x\}$, which is the same as for all $x \neq y \in C$, $\Delta(x,y) \geq t+1$. We see that

$$\Delta(0000, 0011) = 2$$
$$\Delta(0000, 1100) = 2$$
$$\Delta(0011, 1100) = 4,$$

thus $\Delta(x,y) \geq 2$ for all $x \neq y \in C$. Therefore, the code is 1-error detecting.

Let $d(C) = \min_{x \neq y \in C} \Delta(x,y)$. A code C is t-error correcting if $d(C) \geq 2t+1$. In our case $\Delta(C) = 2$, thus there are no positive t which fulfill $2t+1 \leq d(C) = 2$. So C is not an error correcting code.
(4) We have that $q = 3$,$n = 4$, $t = 1$. Thus,

$$|C| \leq \frac{3^4}{\sum_{i=0}^{1} \binom{4}{i}(3-1)^i} = \frac{3^4}{\binom{4}{0}(2)^0 + \binom{4}{1}(2)} = \frac{3^4}{1+8} = 9.$$

Problem 13.1.

(1) Let $A = \{0,1\}, n \geq 0$. Elements of A^n are identified with the vertices of the hypercube graph Q_n. Show that for words $w_1, w_2 \in A^n$, the Hamming distance $\Delta(w_1, w_2)$ equals the path-length distance $d(w_1, w_2)$ in Q_n.
(2) Let $A = \{0, 1, \ldots k\}, n \geq 0$. Show that there is a graph G with vertex set A^n such that for $w_1, w_2 \in A^n$, we have $\Delta(w_1, w_2) = d_G(w_1, w_2)$. Draw this graph when $k = n = 2$.

Solution.

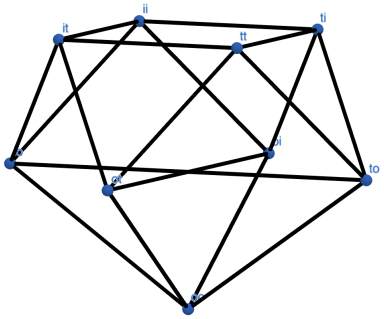
(1) First we show that $d(w_1, w_2) \leq \Delta(w_1, w_2)$ and then that $d(w_1, w_2) \geq \Delta(w_1, w_2)$.

Assume that $\Delta(w_1, w_2) = k$. This means that w_1 and w_2 differ in exactly k positions. We can go from w_1 to w_2 in the hypercube by changing one bit in w_1 in every step. This will make a path of length k, thus $d(w_1, w_2) \leq \Delta(w_1, w_2)$.

On the other hand, let l be a path from w_1 to w_2 in the hypercube. In each step of the path we change one position of w_1, since vertices in Q_n are incident only if they differ in one position. Since we have to change at least k positions to go from w_1 to w_2, we have $d(w_1, w_2) \geq \Delta(w_1, w_2)$. This shows that $d(w_1, w_2) = \Delta(w_1, w_2)$.

(2) We define the edge set $E(G)$ such that there is an edge between two elements $w_1, w_2 \in A$ if w_1 and w_2 differ in exactly one position. The proof that $\Delta(w_1, w_2) = d_G(w_1, w_2)$ is similar to point (1).

The graph when $k = n = 2$ ($(o = 0, i = 1, t = 2)$):



Problem 13.2. Let $A = \{0, 1\}, n \geq 1$.

(1) Recall the **binary checksum code** $C \subseteq A^n$, consisting of all words with an even number of 1s.
   (a) Prove that if $n = 1$, then C is 1-perfect.
   (b) Prove that if $n \geq 2$, then C is not t-perfect for any t.

(2) Recall the **double repetition code** $C \subseteq A^{3n}$, consisting of all length n words repeated twice, that is

$$C = \{www | w \in A^n\}.$$

   (a) Prove that if $n = 1$, then C is 1-perfect.
   (b) Prove that if $n \geq 2$, then C is not t-perfect for any t.

Solution.

(1) (a) Let $n = 1$, thus $C \subset A^1 = \{0, 1\}$. The claim that $C = \{0\}$. Indeed, 0 consists of zero 1s, thus an even number of 1s, and 1 consists of one 1, thus an odd number of 1s. Now, we compute the Hamming bound of C to check that C is 1-perfect. We have that $q = 2$, $n = 1, t = 1$.

$$\frac{2^1}{\binom{1}{0}(2-1)^0 + \binom{1}{1}(2-1)^1} = \frac{2}{1+1} = 1.$$

Since $|C| = 1$, we have that $|C|$ is equal to the Hamming bound, thus C is 1-perfect. *The condition that $d(C) \geq 2t+1$ does not apply in this case since $d(C)$ is not defined (or is defined to be ∞).*

(b) Let $n \geq 2$. First, we compute the Hamming bound

$$\frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}(2-1)^i} = \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}.$$

Next, we compute $|C|$. The number of words of length n with an even number of 1s is the same as the number of words of length n with an odd number of 1s. Thus, $|C| = \frac{1}{2}2^n = 2^{n-1}$. Now, we need to show that

$$|C| = 2^{n-1} \neq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}},$$

but this is the same as showing that

$$\sum_{i=0}^{t} \binom{n}{i} \neq 2.$$

If $t = 1$, we have $\sum_{i=0}^{t} \binom{n}{i} = 1+n$ which is not equal to 2 since we have assumed $n \geq$. If $t > 1$, the sum consist of more positive summands, thus the sum is bigger. This shows that

$$\sum_{i=0}^{t} \binom{n}{i} \neq 2.$$

for $t \geq 1$.

(2) (a) Let $n = 1$. Then $C = \{000, 111\}$, thus $|C| = 2$. We compute the Hamming bound. We have that $q = 2, n = 3, t = 1$.

$$\frac{2^3}{\binom{3}{0}(2-1)^0 + \binom{3}{1}(2-1)^1} = \frac{8}{1+3} = 2.$$

(b) Let $n \geq 2$. First, we compute $d(C)$.

$$\begin{aligned} d(w_1w_1w_1, w_2w_2w_2) &= d(w_1, w_2) + d(w_1, w_2) + d(w_1, w_2) \\ &= 3d(w_1, w_2) \\ &= 3 \cdot 1 \\ &= 3. \end{aligned}$$

Thus, $d(C) = 3 \geq 2t + 1$, so $t \leq 1$. This means that we only have to check that C is not 1-perfect. Next, we find $|C|$. Since there are 2^n elements in A^n, there are also 2^n elements in C, thus $|C| = 2^n$. Now, we compute the Hamming bound.

$$M = \frac{(2^n)^{3n}}{\binom{3n}{0}(2^n-1)^0 + \binom{3n}{1}(2^n-1)^1} = \frac{8^{n^2}}{1+3n(2^n-1)}.$$

This expression is not equal to 2^n, thus $|C| \neq M$.

Week of 28 April – Linear codes (and a little more on general codes)

Warm-ups.

(1) Consider the code
$$C = \{0000, 0101, 1010, 1111\} \subseteq \mathrm{GF}(2)^4.$$
Explain why C is linear, and write down a generator matrix G and a parity matrix H for it.

(2) Can a code $C \subseteq \{0,1\}^n$ with $|C| = 9$ be linear, where $\{0,1\} = \mathrm{GF}(2)$?

Solution.

(1) C is a linear code if it is a subspace of $\mathrm{GF}(2)^4$. Thus, we must have $0000 \subset C$ and C must be closed under vector addition. We check the last property.
$$0101 + 1010 = 1111$$
$$0101 + 1111 = 1010$$
$$1010 + 1111 = 0101$$
This shows that C is closed under vector addition.

Since 0101 and 1010 are linearly independent and generate C, they form a basis for C. Thus,
$$G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

The parity matrix H is such that $Hc = 0$ for $c \in C$. It is enough to check this on the basis. Thus, we must have
$$\begin{pmatrix} h_{11} & h_{12} & h_{13} & h_{14} \\ h_{21} & h_{22} & h_{23} & h_{24} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} h_{11} + h_{13} & h_{12} + h_{14} \\ h_{21} + h_{23} & h_{22} + h_{24} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
Thus,
$$h_{11} = h_{13}$$
$$h_{12} = h_{14}$$
$$h_{21} = h_{23}$$
$$h_{22} = h_{24}$$
We see that these equations are fulfilled if we set $H = G$. Thus
$$H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

(2) We claim that a linear code $C \subseteq \mathrm{GF}(2)^n$ has 2^k code words, for $k \in \mathbb{N}$. Indeed, let $g_1, \ldots, g_k$ be the basis of C. Since C should be closed under vector addition, the words in C is on the form
$$a_1 g_1 + a_2 g_2 + \cdots + a_k g_k,$$

where $a_i \in \mathrm{GF}(2)$. Since each a_i can be either 0 or 1, there are 2^k such words. Thus, $|C| = 2^k$. Since 9 is not a power of 2, there are no code such code C with $|C| = 9$.

Problem 14.1.

(1) Show that if $C \subseteq \{0,1\}^8$ is a 2-error correcting linear code, then $|C| \leq 4$.
(2) Describe a linear code C with $|C| = 4$ which is 2-error correcting.

Solution.

(1) We use the Hamming bound to find that $|C| \leq 6$. Since C should be linear, we use that $|C|$ must be a power of 2 as we showed in warm-ups (2). Thus, $|C| \leq 4$.
(2) Since $|C| = 4 = 2^2$, the basis of C must consist of two code words. Since C should be 2-error correcting, $d \geq 2 \cdot 2 + 1 = 5$. We claim that $g_1 = (1,1,1,1,1,0,0,0)$ and $g_2 = (0,0,0,1,1,1,1,1)$ generates such a code. Indeed, then $C = \{00000000, 11111000, 00011111, 11100111\}$, where the generators have weight 5 and the last word has weight 6. Thus, $d = 5$.

Problem 14.2. Let $A = \mathrm{GF}(11)$, and consider the linear code $C \subseteq A^{11}$ determined by the parity checksum matrix

$$\begin{pmatrix} 3 & 7 & 6 & 1 & 8 & 9 & 4 & 5 & 2 & 1 & 0 \\ 5 & 4 & 3 & 2 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

A Norwegian personal identity number is a string of 11 digits $a_1 a_2, \ldots a_{11}$ which must satisfy $(a_1, \ldots, a_{11}) \in C$.

(1) Find the dimension of C, the cardinality $|C|$, and $d(C)$. Determine for what t the code C is t-error correcting and t-error detecting.
(2) Find two elements $\overrightarrow{a}, \overrightarrow{b} \in C$ such that $\Delta(\overrightarrow{a}, \overrightarrow{b}) = d(C)$.

Solution.

(1) We have that G is an $n \times k$ matrix and H is an $(n-k) \times n$ matrix. Since H is an 2×11 matrix, we get that $n = 11, k = 9$. Thus, C has 9 basis elements and therefore dimension 9.

The number of elements in C is the number of vectors we can make from combining the 9 basis vectors with coefficients from A. Thus, $|C| = 11^9$.

To find $d(C)$ we use Theorem 13.5 which says that $d(C) \geq d$ if and only if every $d-1$ columns in H are linearly independent. Since the 4th and the 10th column are equal, we don't have that every 2 columns are linearly dependent. Since every column in H are not a scalar multiple of one another, we have that every $d - 1 = 1$ column(s) in H are linearly independent, but not 2, thus $d(C) \geq 2$ and $d(C) < 3$. Thus, $d(C) = 2$. Since $d(C) = 2$, C is not error correcting, but 1-error detecting.
(2) We use that the 4th and the 10th column in H are the same, thus if $\overrightarrow{a} = (0,0,0,1,0,0,0,0,0,-1,0)$ then $H\overrightarrow{a} = 0$. Since $-1 = 10 \pmod{11}$, $\overrightarrow{a} = (0,0,0,1,0,0,0,0,0,10,0)$. Since $\overrightarrow{a}$ has weight 2, we choose $\overrightarrow{b} = (0,0,0,0,0,0,0,0,0,0,0)$ and get $\Delta(\overrightarrow{a}, \overrightarrow{b}) = 2$.

Problem 14.3. Let $(S, \mathcal{B})$ be a t-design with $S = \{1, \dots, v\}, |B| = k$ for all $B \in \mathcal{B}$, and $\lambda = 1$. Define a code

$$C = \{c_B \mid B \in \mathcal{B}\} \subseteq \{0,1\}^v,$$

where c_B is the vector of zeros and ones with the ith coordinate equal to 1 if $i \in B$ and 0 otherwise.

(1) What is $|C|$?
(2) Show that for $B_1, B_2 \in \mathcal{B}$,

$$\Delta(c_{B_1}, c_{B_2}) = |B_1 \setminus B_2| + |B_2 \setminus B_1|$$

(3) Show that $d(C) \geq 2(k - t + 1)$.

Solution.

(1) Since C consists of one element for each element $B \in \mathcal{B}$, $|C| = |\mathcal{B}| = k$.
(2) The distance between c_{B_1} and c_{B_2} is the number of positions where they differ. They differ in the ith position if $i \in B_1$ and $i \notin B_2$ or $i \notin B_1$ and $i \in B_2$. The number of such is is $|B_1 \setminus B_2| + |B_2 \setminus B_1|$.
(3) We have that $d(C) = \min_{c_{B_1} \neq c_{B_2}} \Delta(c_{B_1}, c_{B_2}) = \min_{c_{B_1} \neq c_{B_2}} |B_1 \setminus B_2| + |B_2 \setminus B_1|$. Further, we have that $|B_1 \setminus B_2| + |B_2 \setminus B_1| = |B_1| + |B_2| - 2|B_1 \cap B_2| = 2(k - |B_1 \cap B_2|)$. We claim that $|B_1 \cap B_2| \leq t - 1$. Indeed, since $(S, \mathcal{B})$ is a t-design with $\lambda = 1$, a t-subset is contained in exactly one B. Thus, $|B_1 \cap B_2| \leq t - 1$. This shows that

$$d(C) = \min_{c_{B_1} \neq c_{B_2}} \Delta(c_{B_1}, c_{B_2}) = \min_{c_{B_1} \neq c_{B_2}} 2(k - |B_1 \cap B_2|) \geq 2(k - t + 1)$$

Problem 14.4. Prove that the Hamming distance satisfies the triangle inequality, namely

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

for all $a, b, c \in A^n$.

Solution. Assume i such that $a_i = c_i$. Then this position does not contribute to $\Delta(a, c)$. If also $b_i = a_i = c_i$, then the ith position does not contribute to $\Delta(a, b)$ and $\Delta(b, c)$ neither. If $b_i \neq a_i$, this position contributes to both $\Delta(a, b)$ and $\Delta(b, c)$. Thus in either case, the left side is less than or equal to the right side.

Assume i such that $a_i \neq c_i$. Then the ith position contributes with 1 to $\Delta(a, c)$. Then $b_i \neq a_i$ and/or $b_i \neq c_i$. Thus the ith position contributes to the right side with either 1 or 2. We can't have that $b_i = a_i$ and $b_i = c_i$ since $a_i \neq c_i$. We have analysed each case and shown that the left side s greater than or equal to the right side.

Problem 14.5. Consider the vectors $c = (0, 1, 1, 2)$ and $c' = (1, 0, 1, 1)$ in GF(3). The linear code $C \subseteq \mathrm{GF}(3)^4$ generated by c and c' consists of all linear combinations over GF(3) of c and c'.

(1) Write down the list of code words in C and verify that $d(C) = 3$.
(2) Show that C is 1-perfect.

Solution.

(1) The code words in C is the elements $a_1c + a_2c'$ where $a_1, a_2 \in \mathrm{GF}(3)$. This gives the following code words

$$\begin{aligned}
0 \cdot (0,1,1,2) + 0 \cdot (1,0,1,1) &= (0,0,0,0)\\
1 \cdot (0,1,1,2) + 0 \cdot (1,0,1,1) &= (0,1,1,2)\\
1 \cdot (0,1,1,2) + 1 \cdot (1,0,1,1) &= (1,1,2,0)\\
1 \cdot (0,1,1,2) + 2 \cdot (1,0,1,1) &= (2,1,0,1)\\
2 \cdot (0,1,1,2) + 0 \cdot (1,0,1,1) &= (0,2,2,1)\\
2 \cdot (0,1,1,2) + 1 \cdot (1,0,1,1) &= (1,2,0,2)\\
2 \cdot (0,1,1,2) + 2 \cdot (1,0,1,1) &= (2,2,1,0)\\
0 \cdot (0,1,1,2) + 1 \cdot (1,0,1,1) &= (1,0,1,1)\\
0 \cdot (0,1,1,2) + 2 \cdot (1,0,1,1) &= (2,0,2,2)
\end{aligned}$$

We verify that $d(C) = 3$ by checking the distances between pairs of the words.

(2) We check that

$$|C| = \frac{q^n}{\binom{n}{0}(q-1)^0 + \binom{n}{1}(q-1)^1} = \frac{q^n}{1 + n(q-1)}$$

We have that $|C| = 9$, $q = 3$, $n = 4$ and get

$$\frac{q^n}{1+n(q-1)} = \frac{3^4}{1+4(3-1)} = \frac{3^4}{9} = 9 = |C|.$$

Week of 5 May – More linear codes and cyclic codes

Warm ups.

(1) Write down the polynomial for the code word $(1,2,0,1,2) \in \mathrm{GF}(3)$.
(2) Is the binary code $\{0000, 1100, 0110, 0011\}$ cyclic?
(3) What is the dimension of the cyclic code C with generating polynomial $g(x) = x - 1$?
(4) Is there a cyclic code $C \subset \mathrm{GF}(3)^5$ with generating polynomial $g(x) = x+1$?

Solution.

(1) We write $(1,2,0,1,2) = (a_4, a_3, a_2, a_1, a_0)$, thus

$$a(x) = \sum_{i=0}^{4} a_i x^i = x^4 + 2x^3 + x + 2.$$

(2) No. Let $c = (1100)$. Then $\hat{c} = (1001) \notin C$.
(3) We have that $\dim C = n - \deg(g(x))$. By Theorem 13.10, $g(x)$ should divide $x^n - 1$. Since $g(x) = x - 1$, this is fulfilled for any n. Thus, $\dim C = n - 1$, for $C \in K^n$.
(4) We use Theorem 13.10, and have to check if $g(x)$ divides $x^5 - 1$. Since $(-1)^5 - 1 = -2 \equiv 1 \pmod 3$, $g(x)$ does not divide $x^5 - 1$, so there isn't a cyclic code $C \subset \mathrm{GF}(3)^5$.

Problem 15.1. Consider the linear code $C \subseteq \mathrm{GF}(3)^5$ given by the check matrix

$$H = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

(1) Find a generating matrix of C.
(2) Show that C is 1-error correcting.
(3) Suppose the message 21012 was received over a channel with at most one error. Find the syndrome and correct the error.

Solution.

(1) Since H is a 3×5 matrix, G^T is a 5×2 matrix, thus C has two generators. We need two linearly independent vectors c_1, c_2 such that $Hc_1 = Hc_2 = 0$. Two such vectors are $c_1 = (11111)$ and (12120), thus

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 & 0 \end{pmatrix}.$$

(2) For C to be 1-error correcting, we must have $d(C)2 \cdot 1 + 1 = 3$. We use Theorem 13.5 to check that $d(C) \geq 3$. The theorem says that $d(C) \geq 3$ if and only if every 2 columns in H are linearly independent. Since none of the columns in H are a multiple of one of the other columns, every 2 columns in H are linearly independent.
(3)

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$

Thus, the syndrome is $(2, 0, 0)$. Since $(2, 0, 0)$ is a multiple of the first column in H, the error occurred in the first position. Thus, the correct message is

$$(21012) - (20000) = (01012).$$

Problem 15.2. Show that in a linear code C over $\mathrm{GF}(2)$, either all codewords have even weight or half have even weight and half odd weight.

Solution. Let $u, v \in C$. If both u and v has even length or both has odd length, then $u + v$ has even length, and if one of u and v has even length and one has odd length, then $u + v$ has odd length (convince yourself by computing some examples).

Assume that at least one code word has odd weight, say $u \in C$. Let $F_u : C \to C$ be a map such that $v \mapsto u + v$. Thus, if v has even weight, $u + v$ has odd weight, and if v has odd weight, $u + v$ has even weight. We claim that F_u is a bijection. To show that F_u is injective, we see that if $u + v_1 = u + v_2$, then $v_1 = v_2$. To show that F_u is surjective, let $w \in C$. Then $F_u(u - w) = u + (u - w) = w$, thus F_u is surjective. Since F_u is a bijection and maps a code word of odd weight to a code word of even weight, and a code word of even weight to a code word of odd weight, there must be the same number of code words of even weight and of odd weight.

If there is no code word with odd weight, then all code words has even weight.

Problem 15.3. Let $C \subseteq \mathrm{GF}(2)^7$ be the cyclic code generated by $g(x) = x^3+x^2+1$.

(1) Find a generating matrix and the parity check matrix of C.
(2) Is the word $c = (1,1,1,0,1,0,1)$ in C?
(3) Find the syndrome of c with respect to the parity check matrix.

Solution.

(1) We follow the description on page 295 and get

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

We use the factorization of $x^7 - 1$ in Example 13.11, and get that

$$\begin{aligned} h(x) = \frac{x^7-1}{x^3+x^2+1} &= \frac{(x+1)(x^3+x+1)(x^3+x^2+1)}{x^3+x^2+1} \\ &= (x+1)(x^3+x+1) \\ &= x^4+x^3+x^2+1 \end{aligned}$$

Thus,

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

(2) We check if $Hc = 0$:

$$\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

(3) The syndrome of c is (101).

Problem 15.4. Show that the dual code of a cyclic code is cyclic.

Solution. Recall that

$$C^\perp = \{a \in K^n \ : \ a \cdot c = 0 \text{ for all } c \in C\}.$$

We have to show that if C is cyclic, then for any $c' = (c'_{n-1}, \dots, c'_0) \in C^\perp$, also $(c'_{n-2}, \dots, c'_0, c'_{n-1}) \in C^\perp$. Let $c \in C$ be such that $c \dots c' = 0$, that is

$$c \cdot c' = (c_{n-1}, \dots, c_0) \cdot (c'_{n-1}, \dots, c'_0) = c_{n_1} \cdot c'_{n-1} + \cdots + c_0 \cdot c'_0 = 0.$$

Let $c_1 = (c_{n_2}, \dots, c_0, c_{n_1})$. Since C is cyclic, $c_1 \in C$. We claim that

$$c_1 \cdot (c'_{n-2}, \dots, c'_0, c'_{n-1}) = 0$$

which shows that $(c'_{n-2}, \ldots, c'_0, c'_{n-1}) \in C^\perp$ and $C^\perp$ is cyclic. Indeed,

$$\begin{aligned}(c_{n-2}, \ldots, c_0, c_{n-1}) \cdot (c'_{n-2}, \ldots, c'_0, c'_{n-1}) &= c_{n-2} \cdot c'_{n-2} + \cdots + c_0 \cdot c'_0 + c_{n-1} \cdot c'_{n-1} \\ &= c \cdot c' \\ &= 0.\end{aligned}$$

Problem 15.5. Let C_1 and C_2 be two cyclic codes over $\mathrm{GF}(q)$ with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Show that $C_1 \subseteq C_2$ if and only if $g_2(x)$ divides $g_1(x)$.

Solution. Assume that $g_2(x)$ divides $g_1(x)$, that is $g_1(x) = m(x)g_2(x)$ for a polynomial $m(x)$. Let $c_1 \in C_1$. Then there exists $p(x)$ such that $g_1(x)p(x) = c_1(x)$. Using that $g_2(x)$ divides $g_1(x)$ we have that $c_1(x) = m(x)p(x)g_2(x)$, thus $c_1 \in C_2$.

For the other direction we prove that if $g_2(x)$ does not divide $g_1(x)$, then $C_1 \nsubseteq C_2$. Let $g_1 \in C_1$ be the element in C_1 corresponding to $g_1(x)$. Since $g_2(x)$ does not divide $g_1(x)$, $g_1 \notin C_2$. Thus, $C_1 \nsubseteq C_2$.

We can also prove the last direction with a direct proof. Assume $C_1 \subseteq C_2$ and let $g_1 \in C_1$ as above. Then also $g_1 \in C_2$ by assumption. Since $g_1 \in C_1$, $g_2(x)$ divides $g_1(x)$.

Problem 15.6. Let $f(x), g(x)$ be polynomials over $\mathrm{GF}(q)$ of degree less than n, and let $\overrightarrow{f}, \overrightarrow{g} \in \mathrm{GF}(q)^n$ be the associated code words. Prove that if

$$f(x^{-1})g(x) = \sum_{i=-n+1}^{n-1} c_l x^l \qquad c_l \in \mathrm{GF}(q)$$

then

$$\overrightarrow{f} \cdot \overrightarrow{g} = c_0.$$

Solution. Let $\overrightarrow{f} = (f_{n-1}, f_{n-2}, \ldots, f_1, f_0)$ and $\overrightarrow{g} = (g_{n-1}, g_{n-2}, \ldots, g_1, g_0)$. Then

$$\overrightarrow{f} \cdot \overrightarrow{g} = f_{n-1}g_{n-1} + f_{n-2}g_{n-2} + \cdots + f_1 g_1 + f_0 g_0$$

We want to show that this is equal to c_0. We write out $f(x^{-1})g(x)$.

$$f(x^{-1})g(x) = (f_0 + f_1 x^{-1} + \cdots + f_{n-1}x^{-(n-1)})(g_0 + g_1 x + \cdots + g_{n-1}x^{n-1})$$

We have that c_0 is the constant part of $f(x^{-1})g(x)$. Since $x^k \cdot x^{-k} = x^0 = 1$, we get that

$$c_0 = f_0 g_0 + f_1 g_1 + \cdots + f_{n-2}g_{n-2} + f_{n-1}g_{n-1}.$$

Problem 15.7. Let $K = \mathrm{GF}(q)$, and say that a vector $\overrightarrow{a} \in K^m$ is **normalized** if $\overrightarrow{a} \neq \overrightarrow{0}$ and the first non-zero component of $\overrightarrow{a}$ is 1, i.e. we have

$$\overrightarrow{a} = (0, \ldots, 0, 1, a_{i+1}, \ldots, a_m).$$

(1) Prove that if $\overrightarrow{a} \neq \overrightarrow{b}$ and both $\overrightarrow{a}$ and $\overrightarrow{b}$ are normalized, then $\overrightarrow{a}$ and $\overrightarrow{b}$ are linearly independent.
(2) Find the number of normalized vectors in K^m.
(3) Let H be a matrix whose columns are all the normalized vectors of K^m. Explain why the code C with parity check matrix H is a Hamming code.

Solution.

(1) Let i, j be such that $\overrightarrow{a}$ has the first non-zero component in the ith position and $\overrightarrow{b}$ has the first non-zero component in the jth position. Assume $i < j$. Then $\overrightarrow{b}$ has a zero in the ith position. Since $\overrightarrow{a}$ has 1 and $\overrightarrow{b}$ has 0 in the ith position, they cannot be linearly independent. Assume now that $i = j$. Then both $\overrightarrow{a}$ and $\overrightarrow{b}$ has a 1 in the ith position. Thus, $\overrightarrow{a}$ and $\overrightarrow{b}$ is linearly dependent only if they are equal, but we assumed $\overrightarrow{a} \neq \overrightarrow{b}$, so they are not linearly dependent.

(2) If the first non-zero element is in the ith position, there are q^{m-i} possibilities for the remaining entries. Since $1 \leq i \leq m$, we have that the number of normalized vectors in K_m is $\sum_{i=1}^{m} q^{m-i}$. We compute the sum

$$\sum_{i=1}^{m} q^{m-i} = \sum_{i=0}^{m-1} q^i = \frac{q^m - 1}{q - 1},$$

where we have used the formula for the sum of a geometric series.

(3) A Hamming code is a 1-perfect code. First, we need to show that $d(C) \geq 2 \cdot 1 + 1 = 3$. From Theorem 13.5, we have that $d(C) \geq 3$ if and only if every pair of columns in H are linearly independent. We showed in (1) that this is the case. Further, we have to show that $|C|$ is equal to the Hamming bound. Since H is an $m \times \frac{q^m-1}{q-1}$, matrix, the number of generators in C are $\frac{q^m-1}{q-1} - m$. The number of elements in C is then $q^{\frac{q^m-1}{q-1}-m}$. The length of each code word in C is $\frac{q^m-1}{q-1}$.

The Hamming bound is

$$\frac{q^{\frac{q^m-1}{q-1}}}{1 + \frac{q^m-1}{q-1}(q-1)} = \frac{q^{\frac{q^m-1}{q-1}}}{q^m} = q^{\frac{q^m-1}{q-1}-m} = |C|.$$

Week of 12 May – Cryptography

Warm ups.

(1) Show that 2 is a primitive root $\pmod 5$.
(2) Compute $2^{103} \pmod 5$ using Fermat's little theorem.
(3) Compute $3^7 \pmod{11}$ and $3^8 \pmod{11}$ using the successive square method.

Solution.

(1) We have that

$$\begin{aligned} 2^1 &\equiv 2 \pmod 5 \\ 2^2 &\equiv 4 \pmod 5 \\ 2^3 &\equiv 1 \pmod 5 \\ 2^4 &\equiv 3 \pmod 5 \end{aligned}$$

Since all above is incongruent modulo 5, 2 is a primitive root $\pmod 5$.

(2) From Fermat's little theorem we have that $2^{5-1} = 2^4 \equiv 1 \pmod 5$. Thus,

$$\begin{aligned} 2^{103} = 2^{4\cdot 25+3} = 2^{4\cdot 25} \cdot 2^3 &\equiv 1^{25} \cdot 2^3 \pmod 5 \\ &\equiv 3 \pmod 5. \end{aligned}$$

(3) We follow the steps in the method.
- (1) $7 = 2^0 + 2^1 + 2^2$.
  (2)
$$3^{2^0} = 3^1 = 3$$
$$3^{2^1} = 3^2 = 9$$
$$3^{2^2} = 3^4 = 81 \equiv 4 \pmod{11}$$
  (3) $3 \cdot 9 \cdot 4 \equiv 1 \cdot 9 \pmod{11} \equiv 9 \pmod{p}$.
- (1) $8 = 2^3$
  (2) $3^{2^3} = 3^4 \cdot 3^4 = 81 \cdot 81 \equiv 4 \cdot 4 \pmod{11} \equiv 5 \pmod{11}$.
  (3) In this case the last step is the same as step 2 since 8 is a power of 2, thus $3^8 \equiv 5 \pmod{5}$.

Problem 16.1. Solve the discrete logarithm problem

$$3 \equiv 7^x \pmod{11}$$

for $x \in \{0, 1, \ldots, 10\}$.

Solution.

$$7^0 \equiv 1 \pmod{11}$$
$$7^1 \equiv 7 \pmod{11}$$
$$7^2 = 49 \equiv 5 \pmod{11}$$
$$7^3 \equiv 5 \cdot 7 \pmod{11} \equiv 2 \pmod{11}$$
$$7^4 = 5 \cdot 5 \pmod{11} \equiv 3 \pmod{11}$$

Since $7^4 \equiv 3 \pmod{11}$, $x = 4$. Since the discrete logarithm problem is defined for primitive root, the problem has only one solution. Thus, $x = 4$ is the only solution.

Problem 16.2. Let a be a primitive root $\pmod{p}$, let $b = a^k \pmod{p}$, and let $d = \gcd k, p - 1$.

(1) With $m \geq 0$, show that $a^m \equiv 1 \pmod{p}$ if and only if $p - 1$ divides m.
(2) Show that $b^{\frac{p-1}{d}} \equiv 1 \pmod{p}$.
(3) Show that b is a primitive root $\pmod{p}$ if and only if $d = 1$.
(4) Find the number of primitive roots $\pmod{13}$.

Solution.

(1) The case $m = 0$ is straightforward. Assume $m > 0$. For the first direction, assume that $a^m \equiv 1 \pmod{p}$. By the division algorithm, we can write $m = n(p-1) + r$, where $0 \leq r \leq p - 2$. We get

$$a^m = a^{n(p-1)+r} = a^{(p-1)^n} a^r \equiv 1^n a^r \pmod{p} \equiv a^r \pmod{p},$$

where we have used Fermat's little theorem. Since $a^m \equiv 1$ by assumption, $a^r \equiv 1 \pmod{p}$, thus $r = 0$. This shows that $p - 1$ divides m.

For the other direction, assume that $p - 1$ divides m. Thus,

$$a^m = a^{n(p-1)} = a^{(p-1)^n} \equiv 1^n \pmod{p} \equiv 1 \pmod{p}.$$

(2) Let $\frac{k}{d} = l$. We use (1) and get

$$b^{\frac{p-1}{d}} = a^{k\frac{p-1}{d}} = a^{l(p-1)} \equiv 1 \pmod{p}.$$

(3) Assume first that b is a primitive root $\pmod{p}$. Thus, the order of b is $p-1$. This means that $b^n = (a^k)^n = a^{kn} \equiv 1 \pmod{p}$ if and only if $p-1$ divides n. We have shown that $b^{\frac{p-1}{d}} \equiv 1 \pmod{p}$. Thus, $p-1$ divides $\frac{p-1}{d}$. This gives that $d = 1$.

For the other direction, assume $d = 1$. This means that $\gcd(k, p-1) = 1$. Further, we have that $b^n = a^{kn} \equiv 1 \pmod{p}$ if and only if $p-1$ divides kn, since a is a primitive root. Since $d = 1$, $p-1$ have to divide n. This gives that $b^n \equiv 1 \pmod{p}$ if and only if $p-1$ divides n, thus b is a primitive root of p.

(4) First we find one primitive root and then we use the results in this problem to find the remaining. We check if 2 is a primitive root of 13.

$2^1 \equiv 2 \pmod{13}$ $2^2 \equiv 4 \pmod{13}$ $2^3 \equiv 8 \pmod{13}$ $2^4 \equiv 3 \pmod{13}$

$2^5 \equiv 6 \pmod{13}$ $2^6 \equiv 12 \pmod{13}$ $2^7 \equiv 11 \pmod{13}$ $2^8 \equiv 9 \pmod{13}$

$2^9 \equiv 5 \pmod{13}$ $2^{10} \equiv 10 \pmod{13}$ $2^{11} \equiv 7 \pmod{13}$ $2^{12} \equiv 11 \pmod{13}$

Since all the powers are incongruent, 2 is a primitive root of 13. We let $a = 2$ in the results in the problem. Thus every $b = a^k$, where $\gcd(k, p-1) = 1$ is a primitive root. In this case, $p-1 = 12$, and $\gcd(k, 12) = 1$ for $k \in \{5, 7, 11\}$. The remaining primitive roots are

$$2^5 \equiv 6 \pmod{13} \qquad 2^7 \equiv 11 \pmod{13} \qquad 2^{11} \equiv 7 \pmod{13}.$$

Problem 16.3. In a Diffie-Hellman key exchange, Alice and Bob share the public key $p = 11$ and $a = 2$.

(1) Alice sends $A = 10$ to Bob and Bob sends $B = 6$ to Alice. What is their shared secret key K?

(2) The ElGamal protocol encrypts a text T to a cipher

$$C \equiv KT \pmod{p}.$$

Using the ElGamal protocol with their public keys and shared secret, Bob sends the number $C = 6$ to Alice. What was the original number T?

Solution.

(1) First, we need to find Alice's and Bob's private keys x and y. Alice sends Bob $A = a^x \pmod{p}$ and Bob sends Alice $B = a^y \pmod{p}$. Thus

$$A = 10 = 2^x \pmod{11}$$
$$B = 6 = 2^y \pmod{11}$$

We use the table in the book (or the lecture notes) to see that $x = 5$ and $y = 9$. The secret key k fulfil $k = B^x = A^y$. So, Alice computes $B^5 = 6^5 \equiv -1 \pmod{11} \equiv 10 \pmod{11}$ and Bob computes $A^9 = 10^9 = (10^2)^4 10 \equiv (-1)^4 \cdot 10 \pmod{11} \equiv 10 \pmod{11}$. Thus $k = 10$.

(2) We have to solve the equation

$$6 \equiv 10T \pmod{11}$$
$$610^{-1} \equiv T \pmod{11}.$$

Thus, we have to find $10^{-1} \pmod{11}$. We have that

$$\begin{aligned} 10 \cdot 10^{-1} &\equiv 1 \pmod{11} \\ (-1) \cdot 10^{-1} &\equiv 1 \pmod{11} \\ 10^{-1} &\equiv -1 \pmod{11} \end{aligned}$$

Thus, $T \equiv 6 \cdot 10^{-1} \pmod{11} \equiv -6 \pmod{11} \equiv 5 \pmod{11}$.