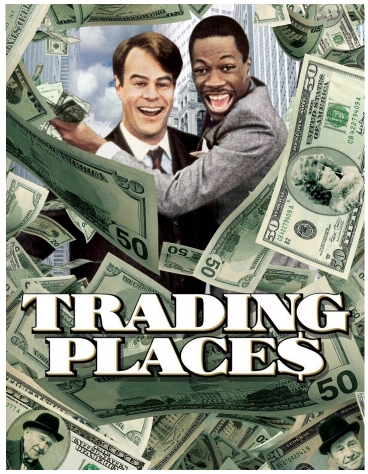
MATH 1800: Quantum Information Theory with Applications to Cryptography

Bonus 4



Stars and bars formula

The number of ways to distribute n indistinguishable objects among k different parties is equal to

$$\binom{n+k-1}{n} = \binom{n+k-1}{k-1}.$$

Proof. Let the objects be represented by stars ($\star$) and the lines of separation between groups by bars ($|$). Thus we need $k-1$ bars. The number of different distributions is the same as the number of different arrangements of n stars and $k-1$ bars, which is equal to $\dfrac{(n+k-1)!}{n!(k-1)!}$. $\square$

$$\underbrace{\star\star\star}_{1^{st}\text{ party}} \; | \; \underbrace{\star\star\star\star}_{2^{nd}\text{ party}} \; | \ldots | \; \underbrace{\star\star}_{k^{th}\text{ party}}$$

Figure 1: Typical arrangement

Definition 1. A polynomial $P(x_1, x_2, \ldots, x_n)$ in n variables is called **homogeneous**, if all nonzero terms of P have the same degree.

A polynomial $P(x_1, x_2, \ldots, x_n)$ in n variables is called **symmetric**, if for any interchange of the variables, one obtains the same polynomial. In a formal language

$$P(x_1, x_2, \ldots, x_n) = P(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})$$

for any permutation σ of the indices $1, 2, \ldots, n$.

Example 2. The polynomials $P_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$, $P_2(x_1, x_2, x_3) = x_1x_2 + x_1x_3 + x_2x_3$ and $P_3(x_1, x_2, x_3) = x_1x_2x_3$ are homogeneous symmetric polynomials of degrees $1, 2$ and 3 in 3 variables.

Problem (4 pts)

(a) Let $k, n \in \mathbb{Z}_{>0}$ be two positive integers. Find the number of ways to write n as a sum of k nonnegative integers.

Example 3. Let $n = 3, k = 2$, then there are 4 ways to decompose 3 into 2 summands:

$$3 = 3 + 0 = 0 + 3 = 2 + 1 = 1 + 2.$$

(b) Find the dimension of the space of homogeneous polynomials of degree n in k variables.

(c) Find the dimension of the space of polynomials of degree less than or equal to n in k variables.[1]

[1]**Hint:** use a dummy variable x_{k+1} and multiply every monomial of degree $s < n$ by x_{k+1}^{n-s}, then use (b).

(d) Let $P(x) = (x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_n)$ be a polynomial with roots $\lambda_1, \lambda_2, \dots, \lambda_n \in \mathbb{C}$. Let's write $P(x)$ in the form $P(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$. Show that the coefficients $a_1, a_2, \dots, a_{n-1}$ are symmetric polynomials in $\lambda_1, \lambda_2, \dots, \lambda_n$ and find these polynomials.[2]

[2] **Hint:** start by working out the examples with $n = 2, 3$.