Exact cover last sequencies
Homework 2 for ITT9131 Concrete Mathematics

Jaan Priisalu

December 20, 2016

1 Exercise 32

32 An *arithmetic progression* is an infinite set of integers

$$\{an + b\} = \{b, a + b, 2a + b, 3a + b, \ldots\}.$$

A set of arithmetic progressions $\{a_1n+b_1\}, \ldots, \{a_mn+b_m\}$ is called an *exact cover* if every nonnegative integer occurs in one and only one of the progressions. For example, the three progressions $\{2n\}$, $\{4n+1\}$, $\{4n+3\}$ constitute an exact cover. Show that if $\{a_1n + b_1\}, \ldots, \{a_mn + b_m\}$ is an exact cover such that

$$2 \leq a_1 \leq \ldots \leq a_m, \text{ then } a_{m-1} = a_m. \tag{1}$$

Hint: Use generating functions.

2 Properties of Polynomials on Complex Plane

Theorem 2.1. *Fundamental Theorem of Algebra: Every non-constant single-variable polynomial with complex coefficients has at least one complex root.*

Proof will not be provided here.

By rules of polynomial division, for every polynomials $f(z)$ and $g(z)$ where $1 < deg\, g \leq deg\, f$, there are unique polynomials $h(z)$ and $r(z)$, with $deg\, r < deg\, h$ such that

$$f(z) = g(z)h(z) + r(z). \tag{2}$$

Equality between polynomials means equality of functions, meaning that they are equal for every value of z

Lemma 2.2. *Every polynomial $f(z)$ can be exatly divided by linear polynomial $z - \varrho$ of it's root $f(\varrho) = 0$.*

Proof. By rule of polynomial division, there are uniqe polynomials h and r with $deg\, r < deg\, h$ such that $f(z) = h(z)(z - \varrho) + r$. As $f(\varrho) = 0$, we have $0 = h(z)0 + r$ and thus $r = 0$. □

Lemma 2.3. *Every polynomial with degree d has exactly d roots*

Proof. Proof by induction. We choose base $d = 1$, then root ϱ_1 is trivial solution of polynomial $z - \varrho_1 = 0$. Induction step. If f(z) is a plynomial of degree $d = n$, that by (2.1) has one root ϱ_n, then we can exactly divide

$$f(z) = (z - \varrho_n)g(z) \tag{3}$$

Degree of $g(z)$ is $n - 1$. □

Polynomial, where coefficent of highest degree of z is 1, we call monic. Monic polynomial can be written as product of linear polynomials of it's root's $f(z) = (z - \varrho_1)(z - \varrho_2)\dots(z - \varrho_n)$.

Root ϱ_i is called multiple root of $f(z)$ if there is another equal root $\exists j \neq i,\ \varrho_j = \varrho_i$.

Lemma 2.4. *Any multiple root ϱ of $f(z)$ is also a root of derivative of $f'(z)$.*

Proof. If $f(z) = (z-\varrho)^2 g(z)$, then we calculate derivative by parts $f'(z) = 2(z-\varrho)g(z) + (z-\varrho)^2 g'(z)$ and therefore $f'(\varrho) = 2(\varrho-\varrho)g(\varrho) + (\varrho-\varrho)^2 g'(\varrho) = 0$. □

3 Complex Roots of 1

For proof of equation (1) with generating functions, we first need to look at properties of polynomials having form

$$1 - z^k\ ,\ where\ k \in N\ . \tag{4}$$

Lemma 3.1. *The polynomial $z^k - 1$ has no multiple root*

Proof. Let ϱ be any root of polynomial $f(z) = z^k - 1$. That means $\varrho^k = 1$ and therefore $\varrho \neq 0$ as $0^k = 0$. Derivative of polynomial is $f'(z) = kz^{k-1}$, let's calculate it at root ϱ, $f'(\varrho) = k\varrho^{k-1} = \frac{k}{\varrho}\varrho^k = \frac{k}{\varrho} \neq 0$. This is true for any root, thus all roots are unique, there is no multiple roots. □

Lemma 3.2. *Polynomial of degree i, $f(z) = z^i - 1$, has a root ϱ, that is not a root of polynomial with lower degree $g(z) = z^j - 1,\ j < i$.*

Proof. Let P be the set of all roots of f $P = \{\varrho_1, \varrho_2, \dots, \varrho_i\}$ and Ω be the set of all roots of g $\Omega = \{\omega_1, \omega_2, \dots, \omega_j\}$. By lemmas (2.3) and (3.1) P has exactly i distinct elements and Ω has exactly j distinct elements. We can bulid correspondence between P and Ω and conclude that there is one root ψ that belongs to P and is not an element of Ω.

$$j < i \ \Rightarrow\ \exists\psi \text{ such that } \psi \in P \text{ and } \psi \notin \Omega. \tag{5}$$

□

4 Proof with Generating Functions

Further we look at generating functions inside convergence radius $|z| < 1$

m *is the number of covering sequencies.*

The sequence of all natural numbers $\{1, 2, 3, \ldots\}$ *is represented by generating function*

$$f(z) = \sum_{j=0}^{\infty} z^j = \frac{1}{1-z} \tag{6}$$

The covering sequencies

$$\{a_j n + b_j\} \; where\, j \in [1, \ldots, m] \tag{7}$$

are represented by generating functions

$$g_j(z) = \sum_{k=0}^{\infty} z^{a_j k + b_j} = \frac{z^{b_j}}{1 - z^{a_j}} \tag{8}$$

As sequencies (7) form exact cover of N *and each natural number is counted exactly once, we can present it's generating function as sum of generating functions of covering sequencies*

$$f(z) = \sum_{j=1}^{m} g_j(z) \tag{9}$$

$$\frac{1}{1-z} = \sum_{j=1}^{m} \frac{z^{b_j}}{1 - z^{a_j}} \tag{10}$$

Now we separate from the sum the last summand

$$\frac{1}{1-z} = \sum_{j=1}^{m} \frac{z^{b_j}}{1 - z_j^a} \tag{11}$$

$$\frac{1}{1-z} = \sum_{j=1}^{m-1} \frac{z^{b_j}}{1 - z_j^a} + \frac{z^{b_m}}{1 - z^{a_m}} \tag{12}$$

$$\frac{z^{b_m}}{1 - z^{a_m}} = \frac{1}{1-z} - \sum_{j=1}^{m-1} \frac{z^{b_j}}{1 - z^{a_j}} \tag{13}$$

Let's look at roots of polynomials in denominators.

First we check the convergence of generating functions.

All they have form (4). The roots are different roots of 1*, solutions of equation* $z^k = 1$*. So all those roots are situated exactly on convergence radius of our generating functions, we can perform calculations as close as needed to the roots from inside the unit circle.*

Proof. Proof by contradiction: we assume

$$a_{m-1} < a_m, \tag{14}$$

that means

$$a_{m-1} \neq a_m. \tag{15}$$

From lemma (3.2), inital condition (1) and our assumption, we know that there exists $\psi^{a_m} = 1$ that is a root of $1 - z^{a_m}$ and is not a root any other polynomial $1-z^{a_i}$, where $i < m$. By construction of sequencies we have $b_m < a_m$ and thus $\psi^{b_m} \neq 0$. We look at the limit, where z closes to ψ, that is on the convergence radius, from inside

$$\lim_{z \to \psi^-} \frac{z^{b_m}}{1 - z^{a_m}} = \frac{\psi^{b_m}}{1 - \psi^{a_m}} = \frac{\psi^{b_m}}{1 - 1} = \infty \tag{16}$$

In the same time, when we look at the limit

$$\lim_{z \to \psi^-} \left(\frac{1}{1 - z} - \sum_{j=1}^{m-1} \frac{z^{b_j}}{1 - z^{a_j}}\right) \tag{17}$$

all summands are finite, there is finte number of summands and therefore this must be also a finite value. Equation (13) must be true everywhere inside the convergence radius and thus we have the contradiction. Therefore our assumption (14) must be wrong and we can deduce $a_{m-1} = a_m$. □