Roots of Unity Filter

Dylan Yu, Raymond Feng

February 14, 2023

Contents

1 Lecture notes

1.1 Statement

A fun story: roots of unity filter (ROUF) was said to be invented by Nikolai Nikolov when he solved IMO 1995/6 in contest via roots of unity. He was awarded a special prize (which is given to people with beautiful solutions) for this discovery.

Theorem 1 (Roots of Unity Filter)
For integers m and n, if we define $\omega = e^{\frac{2\pi i}{n}}$, then the following holds:

$$\sum_{k=0}^{n-1} \left(\omega^k\right)^m = \begin{cases} 0 & n \nmid m \\ n & n \mid m \end{cases}.$$

Proof. Two proofs.

Solution via symmetric sums It suffices to show the result for $0 \leq m < n$, since we may take the exponent mod n without changing the value of the sum. The result is obvious for $m = 0$, so discard that case. Now, as $1, \omega, \omega^2, \ldots, \omega^{n-1}$ are roots of the polynomial $x^n - 1$, this means that all symmetric sums of the nth roots of unity, except for their product, are 0. However, note that the given sum is of degree less than n, so it can be written in terms the symmetric sums without using the product. But all these symmetric sums are 0, so the entire sum evaluates to 0, as desired.

Solution via induction Strong induct on n. The result is obvious for $n = 1$ and n a prime (why?), then split the nth roots of unity into equally spaced groups of size $\frac{n}{\gcd(n,m)}$ and apply the inductive hypothesis to finish. □

1.2 Why is ROUF useful?

The reason: if we have some function[1] $P(x)$, then as the name suggests, by taking $P(1) + P(\omega) + P(\omega^2) + \cdots + P(\omega^{n-1})$, the theorem essentially allows us to *filter* out all coefficients except for those which are a multiple of n. This is why ROUF is usually written in the following form:

Corollary 2 (Alternate Form of ROUF)
Let n be a positive integer, and let $\omega = e^{\frac{2\pi i}{n}}$. For any polynomial $P(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ (with finitely many terms), then

$$a_0 + a_n + a_{2n} + \ldots = \frac{1}{n}\left(P(1) + P(\omega) + P(\omega^2) + \ldots + P(\omega^{n-1})\right).$$

Proof. Left as an exercise; just use the first form of ROUF. □

Remark 3 (Which root of unity?). The nth root of unity we use doesn't have to be $\omega = e^{\frac{2\pi i}{n}}$; it can be ω^k for any k relatively prime to n, but I've never seen a question where ω won't work when ω^k will.

Here is a prototypical example:

Example 4
Evaluate

$$\binom{10}{0} + \binom{10}{2} + \binom{10}{4} + \binom{10}{6} + \binom{10}{8} + \binom{10}{10}.$$

Walkthrough.

1. What should we have as the value of n here? What is our $P(x)$? (Hint: use binomial theorem!)
2. Show that the desired sum is equivalent to $\frac{(1+1)^{10} + (1-1)^{10}}{2}$, and conclude.

The above example uses the 2nd roots of unity, but -1 and 1 aren't enough to justify the use of complex numbers. We'll see a better use of roots of unity in action below.

[1] Usually a rational function, i.e. a polynomial divided by a polynomial.

Example 5
Evaluate
$$\binom{10}{2}+\binom{10}{5}+\binom{10}{8}.$$

Walkthrough.

1. What should we have as the value of n here?
2. Why doesn't the $P(x)$ in our previous problem work? There is an additional reason besides "the common differences are different."
3. How can we edit $P(x)$ so that the coefficients of the terms with degree a multiple of n are precisely $\binom{10}{2}, \binom{10}{5}, \binom{10}{8}$? (Hint: consider dividing by a power of x.)
4. Prove that if $\omega = e^{\frac{2\pi i}{3}}$, then the desired sum is equivalent to
$$\frac{1\cdot(1+1)^{10}+\omega(1+\omega)^{10}+\omega^2(1+\omega^2)^{10}}{3}.$$

Of course, both of the above examples were small enough that they could just be bashed out, but the walkthroughs just serve to illustrate the process of applying the roots of unity filter; the answer extraction is not really the interesting part.

Exercise 6 (Generating function for binomial ROUF). Show that
$$\sum_{k\geq 0}\binom{N}{m+kn}x^{m+kn}=\frac{1}{n}\sum_{k=1}^{n}(\omega^k)^{-m}(1+\omega^k\cdot x)^N,$$
where ω is an nth root of unity.

Moral
The real power of ROUF comes when evaluating how many ways for something to happen such that some parameter is a multiple of some number n. These problems can be tackled using a generating function and then applying ROUF.

For example, the examples above could have instead been rephrased as:

- **Reworded from example 4**: How many ways are there to choose a subset with even size out of 10 distinct objects?
- **Reworded from example 5**: How many ways are there to choose a subset of k objects out of a set of 10 distinct objects such that $k \equiv 2 \pmod 3$?

Although the computations may become very messy in the following problem, can you see the idea behind the solution for it?

Illustrate an idea How many ways are there to choose a subset of k objects out of a set of 2021 distinct objects such that $k \equiv 2 \pmod 3$ or $k \equiv 1 \pmod 4$?

It's just two-set PIE: add the ways for each modulo, then subtract the overlap.

1.3 Themes of ROUF

ROUF is technically an algebraic technique, but its applications to C/G/N are what actually make it useful. In particular, the idea is often to express a non-algebraic problem via the subject's relation to the roots of unity, then use ROUF to do the computation.

Common themes of ROUF: for geometry, it can appear when we're dealing with a regular polygon (because the roots of unity are a regular polygon on the unit circle). For combinatorics and number theory, we'll see it when we're asked to count something constrained by a number-theoretic property, e.g. the large amount of IMO 1995/6 copies.

2 Examples

This next problem is a repeat of the ones before but just for insurance:

Example 7
Compute

$$\sum_{k\geq 0}\binom{1000}{3k}.$$

Walkthrough. Let $f(n)$ equal 1 when $3 \mid n$ and 0 otherwise, and let $\omega = e^{\frac{2\pi i}{3}}$ be a 3rd root of unity.

1. Characterize $f(n)$ with ω.
2. Use $1+\omega+\omega^2 = 0$ to simplify your answer and finish. For example, we can arrange the expression to get $1+\omega = -\omega^2$.

This next example doesn't require roots of unity filter, but when 6 tenors and 8 basses is replaced with a and b of them, respectively, the method becomes more helpful.

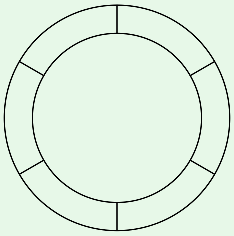
Example 8 (AMC 12A 2021/15)
A choir director must select a group of singers from among his 6 tenors and 8 basses. The only requirements are that the difference between the number of tenors and basses must be a multiple of 4, and the group must have at least one singer. Let N be the number of different groups that could be selected. What is the remainder when N is divided by 100?

Walkthrough. Let $f(x,y) = (1+x)^8(1+y)^6$.

1. Show that coefficient a_{mn} of $x^m y^n$ in the expanded form of f is the number of groups of m basses and n tenors. Thus, we want to sum up all values of a_{mn} for which $4 \mid m-n$, except for $a_{00} = 1$.
2. For what value of y (in terms of x) can we change $x^m y^n$ to x^{m-n}? Let $g(x) = f(x, \bullet)$, where $\bullet$ is the new value of y.
3. Apply ROUF on g with the 4th roots of unity.

Example 9 (AIME II 2016/12)
The figure below shows a ring made of six small sections which you are to paint on a wall. You have four paint colors available and you will paint each of the six sections a solid color. Find the number of ways you can choose to paint the sections if no two

adjacent sections can be painted with the same color.



Walkthrough. Suppose that the colors are $0, 1, 2, 3$. Clearly the difference between the colors in adjacent sections is $1, 2$, or 3 modulo 4. Define the number at each border between sections to be this difference.

1. Use a generating function to represent each border.
2. What is the generating function for all 6 borders then? In this function, the coefficient of x^n should represent the total number of colorings where the colors' numbers are increased by n as we go around the ring.
3. If we go around the ring and the colors have increased by n, what must n be divisible by to ensure that the color of the section we started with is still the right color? Let the number n is divisible by be m.
4. Apply ROUF on $A(x)$ with the mth roots of unity to finish.

See the solutions for other interesting ways of solving the problem, one using linear algebra, and another using chromatic polynomials.

3 Further Reading

1. Things Fourier, Evan Chen
2. Dirichlet's theorem on APs, Evan Chen
3. Cauchy Integral Formula, `Altheman`
4. Generating Functions in CP, `zscoder`
5. More Examples, Kevin Sun
6. Jacobsthal numbers, Wikipedia

4 Problems

Silly example:

Problem 1 (AMC 10B 2021/16). Call a positive integer an *uphill* integer if every digit is strictly greater than the previous digit. For example, 1357, 89, and 5 are all uphill integers, but 32, 1240, and 466 are not. How many uphill integers are divisible by 15?

Problem 2 (BMT Analysis 2015/7). Evaluate $\sum_{k=0}^{37}(-1)^k\binom{75}{2k}$.

Problem 3 (AMC 12A 2017/25). The vertices V of a centrally symmetric hexagon in the complex plane are given by

$$V = \left\{\sqrt{2}i, -\sqrt{2}i, \frac{1}{\sqrt{8}}(1+i), \frac{1}{\sqrt{8}}(-1+i), \frac{1}{\sqrt{8}}(1-i), \frac{1}{\sqrt{8}}(-1-i)\right\}.$$

For each j, $1 \le j \le 12$, an element z_j is chosen from V at random, independently of the other choices. Let $P = \prod_{j=1}^{12} z_j$ be the product of the 12 numbers selected. What is the probability that $P = -1$?

Problem 4. Three regular 7-sided dice, two regular 5-sided dice, and one regular 4-sided die are rolled. The probability that the 6 dice sum to a number divisible by 3 can be expressed as $\frac{m}{n}$, where m and n are relatively prime positive integers. Find m.

Problem 5 (IMC 1999/8). We roll a regular die n times. What is the probability that the sum of the numbers shown is a multiple of 5?

Problem 6 (AIME I 2018/12). For every subset T of $U = \{1, 2, 3, \ldots, 18\}$, let $s(T)$ be the sum of the elements of T, with $s(\emptyset)$ defined to be 0. If T is chosen at random among all subsets of U, the probability that $s(T)$ is divisible by 3 is $\frac{m}{n}$, where m and n are relatively prime positive integers. Find m.

Problem 7 (HMMT February Team 2015/7). Let $f : [0,1] \to \mathbb{C}$ be a *nonconstant* complex-valued function on the real interval $[0,1]$. Prove that there exists $\varepsilon > 0$ (possibly depending on f) such that for any polynomial P with complex coefficients, there exists a complex number z with $|z| \le 1$ such that $|f(|z|) - P(z)| \ge \varepsilon$.

Problem 8 (HMMT February Combinatorics 2012/10). Jacob starts with some complex number x_0 other than 0 or 1. He repeatedly flips a fair coin. If the nth flip lands heads, he lets $x_n = 1 - x_{n-1}$, and if it lands tails he gets $x_n = \frac{1}{x_{n-1}}$. Over all possible choices of x_0; what are all possible values of the probability that $x_{2012} = x_0$?

Problem 9 (Titu). For positive integers n, define

$$f(n) = \sum_{k=0}^{n-1} \cos^{2n}\left(\frac{k\pi}{n}\right).$$

Compute

$$\sum_{k=2}^{\infty} \frac{f(k)}{k \cdot 2^k}.$$

Problem 10 (PUMaC Live 2018/4.3). Let $0 \leq a, b, c, d \leq 10$. For how many ordered quadruples (a, b, c, d) is $ad - bc$ a multiple of 11?

Problem 11 (HMIC 2021/3). Let A be a set of $n \geq 2$ positive integers, and let $f(x) = \sum_{a \in A} x^a$. Prove that there exists a complex number z with $|z| = 1$ and $|f(z)| = \sqrt{n-2}$.

Problem 12 (Putnam 1974/B6). Let S be a set with 1000 elements. Find a, b, c, the number of subsets R of S such that $|R| \equiv 0, 1, 2 \pmod 3$, respectively. Find a, b, c if $|S| = 1001$ instead.

Problem 13 (MOP 1999). There are n points on a unit circle such that the product of the distances from any point on the unit circle to the given points is at most 2. Prove that the given n points must be vertices of a regular n-gon.

5 Selected Solutions

5.1 Solution 4

By binomial theorem,

$$(1+1)^{10} = \sum_{k=0}^{10} \binom{10}{k},$$
$$(1-1)^{10} = \sum_{k=0}^{10} (-1)^k \binom{10}{k},$$

and averaging the two quantities gives us the desired result of $\boxed{512}$.

Remark 10. For reference, we applied ROUF on $P(x) = (1+x)^{10}$, i.e. computed $\frac{P(1)+P(-1)}{2}$.

5.2 Solution 5

Let $\omega = e^{\frac{2\pi i}{3}}$. Then by applying ROUF on $P(x) = x^{-2}(1+x)^{10}$, we note that we have shifted the coefficients by two (i.e. the kth coefficient of $(1+x)^{10}$ is now the $k-2$th coefficient of $x^{-2}(1+x)^{10}$), so $\binom{10}{3k+2}$ for nonnegative integers k are now included in our count. Thus,

$$\begin{aligned}\binom{10}{2} + \binom{10}{5} + \binom{10}{8} &= P(1) + P(\omega) + P(\omega^2) \\ &= 1 \cdot (1+1)^{10} + \omega^{-2}(1+\omega)^{10} + \omega^{-4}(1+\omega^2)^{10}.\end{aligned}$$

Using $\omega^3 = 1$, we get that

$$1 \cdot (1+1)^{10} + \omega(1+\omega)^{10} + \omega^2(1+\omega^2)^{10} = 1026,$$

implying the answer is $\frac{1}{3} \cdot 1026 = \boxed{342}$.

5.3 Solution 7

Solution by Evan Chen.

We can rewrite the sum as

$$\sum_{n \geq 0} \binom{1000}{n} f(n)$$

where

$$f(n) = \begin{cases} 1 & n \equiv 0 \pmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

The trick is that we can take

$$f(n) = \frac{1}{3}\left(1^n + \omega^n + \omega^{2n}\right)$$

where $\omega = e^{\frac{2\pi i}{3}}$ is a cube root of unity, satisfying the relation $\omega^2 + \omega + 1 = 0$. Thus, we have

$$\sum_{n \geq 0} \binom{1000}{n} f(n) = \frac{1}{3} \sum_{n \geq 0} \binom{1000}{n} (1 + \omega^n + \omega^{2n}).$$

We can swap the order of summation now and instead consider

$$\sum_{n\ge 0}\binom{1000}{n}f(n)=\frac{1}{3}\sum_{n\ge 0}\binom{1000}{n}+\frac{1}{3}\sum_{n\ge 0}\binom{1000}{n}\omega^n+\frac{1}{3}\sum_{n\ge 0}\binom{1000}{n}\omega^{2n}.$$

By the binomial theorem, the expression in question is

$$\begin{aligned}\sum_{n\ge 0}\binom{1000}{n}f(n)&=\frac{1}{3}\left[(1+1)^{1000}+(1+\omega)^{1000}+(1+\omega^2)^{1000}\right]\\&=\frac{1}{3}\left[2^{1000}+(-\omega^2)^{1000}+(-\omega)^{1000}\right]\\&=\frac{1}{3}\left[2^{1000}+\omega+\omega^2\right]\\&=\frac{1}{3}\left[2^{1000}-1\right].\end{aligned}$$

5.4 Solution 8 (AMC 12A 2021/15)

Solution by AoPS user `lawliet163`.

Let $f(x,y)=(1+x)^8(1+y)^6$. By expanding the binomials and distributing, $f(x,y)$ is the generating function for different groups of basses and tenors. That is,

$$f(x,y)=\sum_{m=0}^{8}\sum_{n=0}^{6}a_{mn}x^my^n$$

where a_{mn} is the number of groups of m basses and n tenors. What we want to do is sum up all values of a_{mn} for which $4\mid m-n$ except for $a_{00}=1$. To do this, define a new function

$$g(x)=f(x,x^{-1})=\sum_{m=0}^{8}\sum_{n=0}^{6}a_{mn}x^{m-n}=(1+x)^8(1+x^{-1})^6.$$

Now we just need to sum all coefficients of $g(x)$ for which $4\mid m-n$. Consider a monomial $h(x)=x^k$. If $4\mid k$,

$$h(i)+h(-1)+h(-i)+h(1)=1+1+1+1=4$$

otherwise,

$$h(i)+h(-1)+h(-i)+h(1)=0.$$

$g(x)$ is a sum of these monomials so this gives us a method to determine the sum we're looking for:

$$\frac{g(i)+g(-1)+g(-i)+g(1)}{4}=2^{12}=4096$$

(since $g(-1)=0$ and it can be checked that $g(i)=-g(-i)$). Hence, the answer is $4096-1$ with the -1 for a_{00} which gives $\boxed{95}$.

5.5 Solution 9 (AIME II 2016/12)

Three interesting solutions are presented below. You can alternatively do the problem with easier methods, e.g. PIE, casework, or recursion.

Solution via generating functions and ROUF We use generating functions. Suppose that the colors are $0, 1, 2, 3$. Then as we proceed around a valid coloring of the ring in the clockwise direction, we know that between two adjacent sections with colors s_i and s_{i+1}, there exists a number $d_i \in \{1, 2, 3\}$ such that

$$s_{i+1} \equiv s_i + d_i \pmod 4.$$

Thus, we can represent each border between sections by the generating function $x + x^2 + x^3$, where x, x^2, x^3 correspond to increasing the color number by $1, 2, 3 \pmod 4$, respectively. Thus the generating function that represents going through all six borders is

$$A(x) = (x + x^2 + x^3)^6,$$

where the coefficient of x^n represents the total number of colorings where the colors' numbers are increased by a total of n as we proceed around the ring. But if we go through all six borders, we must return to the original section, which is already colored. Therefore, we wish to find the sum of the coefficients of x^n in $A(x)$ with $n \equiv 0 \pmod 4$.

Thus, the sum of the coefficients of $A(x)$ with powers congruent to $0 \pmod 4$ is

$$\frac{A(1) + A(i) + A(-1) + A(-i)}{4} = \frac{3^6 + (-1)^6 + (-1)^6 + (-1)^6}{4} = \frac{732}{4}.$$

We multiply this by 4 to account for the initial choice of color, so the answer is $\boxed{732}$.

Solution via linear algebra (Allen Wang) Consider the graph K_4 and its corresponding adjacency matrix A. The answer to the problem is therefore the trace of A^6 by definition of matrix multiplication. Since $B = A + I$ is a 4×4 matrix full of 1s, B has a rank of 1, and therefore has 3 eigenvalues of 0. Since the trace of B is 4, the last eigenvalue is 4. Thus, A has eigenvalues $-1, -1, -1, 3$.

The trace of A^6 is the sum of the 6th powers of its eigenvalues, so we find that the trace is $3^6 + 3 = \boxed{732}$, as desired.

Solution via chromatic polynomials The chromatic polynomial for a cycle C_n is $(x-1)^n + (-1)^n(x-1)$, where x is the number of colors and n is the number of sections in the cycle. Clearly $x = 4$ and $n = 6$, so the answer is

$$(4-1)^6 + (-1)^6(4-1) = \boxed{732}.$$

> *Remark 11.* Chromatic polynomials are actually what this problem is based on, and thus not the intended solution. Contest problems that can be destroyed with chromatic polynomials usually succumb to casework as well, but I recommend you learn them as they can be useful for timed competitions.