1 Introduction

1.1 Recap: The root of unity filter

Say that we want to figure out what

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + ...$$

is. How might we evaluate this sum?

The answer involves the third root of unity ω, which is a complex number where $\omega^3 = 1$ but $\omega \neq 1$. It satisfies the nice property that

$$\begin{aligned} 1 + 1 + 1 &= 3 \\ 1 + \omega + \omega^2 &= 0 \\ 1 + \omega^2 + \omega^4 &= 0 \\ 1 + \omega^3 + \omega^6 &= 3 \\ &\vdots \end{aligned}$$

So, we can write out the binomial expansion of $(1 + 1)^n$ along with its "root-of-unity-twisted" counterparts:

$$\begin{aligned} (1+1)^2 &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots \\ (1+\omega)^2 &= \binom{n}{0} + \binom{n}{1}\omega + \binom{n}{2}\omega^2 + \binom{n}{3} + \cdots \\ (1+\omega^2)^2 &= \binom{n}{0} + \binom{n}{1}\omega^2 + \binom{n}{2}\omega^4 + \binom{n}{3} + \cdots \end{aligned}$$

Now, by summing these three sums vertically, we get exactly what we want on the RHS, therefore

$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + ... = \frac{2^n + (1+\omega)^n + (1+\omega^2)^n}{3}.$$

The moral of the story here is that

Fact 1 (Root-of-unity filter)

For any positive integer m, n,

$$\frac{1}{n}\sum_{i=1}^{n} e^{2\pi i m/n} = \mathbb{I}_{n|m}$$

where $\mathbb{I}_{n|m}$ is the indicator for $n|m$: 1 if $n|m$ and 0 otherwise.

Odds are that you've tried this problem, but in the off-chance that you have not:

Example 2 (IMO 1995/6)

Let p be an odd prime number. How many p-element subsets A of $\{1, 2, \ldots, 2p\}$ are there, the sum of whose elements is divisible by p?

1.2 More advanced usage

Here we consider two extensions:

1. What if we did the root-of-unity filter on multiple variables?

Example 3 (MPFGO 2016/3)

Let n be a positive integer. Let $x_1, x_2, \ldots, x_n$ be a sequence of n real numbers. Say that a sequence $a_1, a_2, \ldots, a_n$ is unimodular if each a_i is ± 1. Prove that

$$\sum a_1 a_2 \ldots a_n (a_1 x_1 + a_2 x_2 + \cdots + a_n x_n)^n = 2^n n!\, x_1 x_2 \ldots x_n,$$

where the sum is over all 2^n unimodular sequences $a_1, a_2, \ldots, a_n$.

Solution. The key is to understand this sum on monomials:

$$\sum_{a_i \in \{\pm 1\}^n} a_1^{k_1} \cdots a_n^{k_n} = \begin{cases} 2^n & \text{if all } k_i \text{ even,} \\ 0 & \text{otherwise.} \end{cases}$$

This makes it clear that the only terms that don't cancel out are precisely those that get one of each a_i, of which there are $n!$. $\square$

2. Taking "$n \to \infty$" gives us an integral version of the first fact:

Fact 4

For any integer n,

$$\int_0^1 e^{2\pi i n \theta} d\theta = \mathbb{I}_{n=0}$$

Example 5 (Poland Second Round 2023/3, slightly modified)

Let S be a finite set of integers symmetric about 0 (i.e. $x \in S$ iff $-x \in S$). Let n be a positive integer, and for each real number r define A_r to be the set of solutions to

$$x_1 + x_2 + \cdots + x_{2n} = r, \qquad x_i \in S.$$

Prove that $|A_0| \geq |A_r|$ for every $r \neq 0$.

Solution. By direct computation,

$$A = \int_0^1 \left(\sum_{s \in S} e^{2\pi i s \alpha} \right)^{2n} d\alpha$$

and

$$B = \int_0^1 \left(\sum_{s \in S} e^{2\pi i s \alpha} \right)^{2n} e^{-2\pi i \ell \alpha} d\alpha$$

and the claim follows from the triangle inequality, using that $\sum_{s \in S} e^{2\pi i s \alpha} = 2 \sum_{j=1}^{k} \cos(2\pi a_j)$ is real so that the bracketed term is nonnegative (because of the even exponent). $\square$

It's also nice that this classic problem can be solved:

Example 6 (Folklore)

Suppose you can decompose a rectangle into finitely many rectangles, each of which has at least one side of integer length. Then, the original rectangle has at least one side of integer length.

Solution. Set two corners of the rectangle to be $(0,0)$ and (a,b), then note that the integral of $e^{2\pi i(x+y)} dx dy$ over a rectangle is 0 iff the rectangle has at least one side of integer length. Yet, the integral over the big rectangle is the sum of the integrals over the smaller rectangles, so it is also zero. $\square$

To foreshadow a little, we'll sometimes want to do a version of Fact 4 for real numbers, but as it stands it is not true for real values of n. Nonetheless, since the main idea here is that "fluctuations cancel out", we can make it true by instead taking a limit:

Fact 7
Let α be a real number. Then

$$\lim_{T\to\infty} \frac{1}{T} \int_0^T e^{2\pi i \alpha x} dx = \mathbb{I}_{\alpha=0}.$$

2 DFTs and Fourier Analysis

There's an interesting framework to really exploit the above facts, which is the framework of Fourier analysis. For the following discussion, let's look at a sequence of n numbers $a_1, ..., a_n$ and we'll let ω denote a primitive n-th root of unity.

Define the **discrete Fourier transform** of $\{a_i\}$ to be

$$\hat{a}_j = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} \omega^{jk} a_k.$$

There are a few facts that are a good exercise to prove by simply expanding the sums:

Fact 8 (Inverse Fourier Transform)
We can recover a_k from $\hat{a}_j$:

$$a_k = \frac{1}{\sqrt{n}} \sum_{j=1}^{n} \omega^{-jk} \hat{a}_j$$

Fact 9 (Convolutions)
Define

$$(a * b)_m = \sum_{j=1}^{n} a_j b_{m-j}$$

where we take the index mod n. Then $\widehat{a * b} = \hat{a} \cdot \hat{b}$ elementwise.

Fact 10 (Plancherel)
The sum of squared norms of a and $\hat{a}$ are the same, i.e.

$$\sum_{j=1}^{n} |a_j|^2 = \sum_{k=1}^{n} |\hat{a}_k|^2.$$

Fact 11 (Isometry)
If $\langle a, b\rangle := \sum_{i=1}^{n} a_i \overline{b_i}$, then $\langle a, b\rangle = \langle \hat{a}, \hat{b}\rangle$.

Linear algebraic perspective. If you're geometrically minded, all of the above facts might be intuitive. One can think of the function $a \mapsto \hat{a}$ as a linear map with matrix

$$U = \begin{pmatrix} \omega^{0\cdot 0} & \omega^{0\cdot 1} & \cdots & \omega^{0\cdot(n-1)} \\ \omega^{1\cdot 0} & \omega^{1\cdot 1} & \cdots & \omega^{1\cdot(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{(n-1)\cdot 0} & \omega^{(n-1)\cdot 1} & \cdots & \omega^{(n-1)\cdot(n-1)} \end{pmatrix}$$

which satisfies satisfies $UU^\dagger = I$ (with $U^\dagger$ representing the conjugate transpose $(U^\top)^*$). We call such U **unitary**.

From this perspective, it's obvious that (1) we can invert U, (2) U preserves norms and (3) U preserves the conjugate inner product $\langle a, b\rangle = \sum_{i=1}^n a_i\overline{b_i}$.

3 Problems

0. Actually work through the computations for the DFT identities.

1. (2024 Israel TST 6/2) Let n be a positive integer. Find all polynomials $Q(x)$ with integer coefficients so that the degree of $Q(x)$ is less than n and there exists an integer $m \geq 1$ for which
$$x^n - 1 \mid Q(x)^m - 1$$

2. (USEMO 2021/5) Let $S(p)$ denote the sum of the squares of the coefficients of a polynomial $p(x)$. Prove that if $f(x)$, $g(x)$, and $h(x)$ are polynomials with real coefficients satisfying the indentity $f(x) \cdot g(x) = h(x)^2$, then
$$S(f) \cdot S(g) \geq S(h)^2$$

3. (ISL 2018 A6) Let $m, n \geq 2$ be integers. Suppose that $f(x_1, \ldots, x_n)$ is a polynomial with real coefficients such that
$$f(x_1, \ldots, x_n) = \left\lfloor \frac{x_1 + \cdots + x_n}{m} \right\rfloor$$
for every $x_1, \ldots, x_n \in \{0, 1, \ldots, m-1\}$. Prove that the total degree of f is at least n.

4. (Ky Fan's inequality) Let $n \geq 3$ be an integer, and reals $a_1, \ldots, a_n$ sum to zero. Show that
$$\cos \frac{2\pi}{n} \sum_{k=1}^{n} a_k^2 \geq \sum_{k=1}^{n} a_k a_{k+1}.$$

5. (CTST 2020/1) Let ω be a n -th primitive root of unity. Given complex numbers $a_1, a_2, \cdots, a_n$, and p of them are non-zero. Let
$$b_k = \sum_{i=1}^{n} a_i \omega^{ki}$$
for $k = 1, 2, \cdots, n$. Prove that if $p > 0$, then at least $\frac{n}{p}$ numbers in $b_1, b_2, \cdots, b_n$ are non-zero.

6. (HMIC 2017/5, rephrased) Suppose that a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ satisfies $f(s)+f(t) = f(s+t)$ for $(1-\epsilon)$ of all pairs $s, t \in \mathbb{F}_2^n$. Show that there exists a linear map $f' : \mathbb{F}_2^n \to \mathbb{F}_2$ that matches f on at least $(1 - 10\epsilon)$ of the inputs.

7. (CTST 2025/15) Let X be a finite set of real numbers, d be a real number, and $\lambda_1, \lambda_2, \cdots, \lambda_{2025}$ be 2025 non-zero real numbers. Define
   - A to be the set of 2025-tuples $(x_1, x_2, \cdots, x_{2025}) \in X^{2025}$ such that $\sum_{i=1}^{2025} \lambda_i x_i = d$
   - B to be the set of 2024-tuples $(x_1, x_2, \cdots, x_{2024}) \in X^{2024}$ such that $\sum_{i=1}^{2024} (-1)^i x_i = 0$
   - C to be the set of 2026-tuples $(x_1, x_2, \cdots, x_{2026}) \in X^{2026}$ such that $\sum_{i=1}^{2026} (-1)^i x_i = 0$

   Show that $|A|^2 \leq |B| \cdot |C|$.

4 More problems

Some of these problems will need concepts from the appendices.

1. (Erdos-Ginzburg-Ziv) Show that among any $2n-1$ integers, there exists a subset of n integers whose sum is divisible by n.

2. (IMO 2006/6) Assign to each side b of a convex polygon P the maximum area of a triangle that has b as a side and is contained in P. Show that the sum of the areas assigned to the sides of P is at least twice the area of P.

3. (ELMO Shortlist 2023 C8) Let $n \geq 3$ be a fixed integer, and let α be a fixed positive real number. There are n numbers written around a circle such that there is exactly one 1 and the rest are 0's. An operation consists of picking a number a in the circle, subtracting some positive real $x \leq a$ from it, and adding αx to each of its neighbors.

   Find all pairs (n, α) such that all the numbers in the circle can be made equal after a finite number of operations.

4. (Komal A421) Find two positive constants α and c such that

   $$\left|\sum_{k=1}^{N}\left\{\frac{k^2}{N}\right\}-\frac{N}{2}\right| < cN^{1-\alpha}$$

   holds for all positive integers N.

5. (USA TSTST 2018/9) Show that there is an absolute constant $c < 1$ with the following property: whenever $\mathcal{P}$ is a polygon with area 1 in the plane, one can translate it by a distance of $\frac{1}{100}$ in some direction to obtain a polygon $\mathcal{Q}$, for which the intersection of the interiors of $\mathcal{P}$ and $\mathcal{Q}$ has total area at most c.

6. (Brazil Olympic Revenge 2018/5) Let p a prime number and define $\|x\|$ as the cyclic distance of x to 0:

   $$\|x\| = \begin{cases} x & \text{if } x < \frac{p}{2} \\ p-x & \text{if } x > \frac{p}{2} \end{cases}$$

   Let $f : \mathbb{F}_p \to \mathbb{F}_p$ a function such that for every $x, y \in \mathbb{F}_p$

   $$\|f(x+y) - f(x) - f(y)\| < 100$$

   Prove that exist $m \in \mathbb{F}_p$ such that for every $x \in \mathbb{F}_p$

   $$\|f(x) - mx\| < 1000.$$

7. (Canada Training 2024; MO 185278) Show that if G is a subgroup of $\mathbb{F}_p^2$ with $|\mathbb{F}_p^2| \geq p^{(k+1)/2k}$, then every element of $\mathbb{F}_p^2$ is a sum of k elements from G.

8. (ISL 2012 N8) Prove that for every prime $p > 100$ and every integer r, there exist two integers a and b such that p divides $a^2 + b^5 - r$.

9. (RMM 2024/6) A polynomial P with integer coefficients is *square-free* if it is not expressible in the form $P = Q^2R$, where Q and R are polynomials with integer coefficients and Q is not constant. For a positive integer n, let P_n be the set of polynomials of the form

   $$1 + a_1x + a_2x^2 + \cdots + a_nx^n$$

   with $a_1, a_2, \ldots, a_n \in \{0, 1\}$. Prove that there exists an integer N such that for all integers $n \geq N$, more than 99% of the polynomials in P_n are square-free.

10. (China TST 2014/17) Let n be a given integer which is greater than 1 . Find the greatest constant $\lambda(n)$ such that for any non-zero complex $z_1, z_2, \cdots, z_n$,have that

    $$\sum_{k=1}^{n}|z_k|^2 \geq \lambda(n) \min_{1\leq k\leq n}\{|z_{k+1}-z_k|^2\},$$

    where $z_{n+1} = z_1$.

11. (SZM Original NT 137) Let p be a prime number and $n = p - 1$. The sequence $\{a_k\}_{k\in\mathbb{Z}}$ satisfies $a_{k_1} = a_{k_2}$ whenever $k_1 \equiv \pm k_2 \pmod{n}$. If we define

$$D := \gcd_{1\le d\le n}\left(\sum_{k=1}^{n} a_k a_{k+d}\right)$$

show that $v_p(D)$ is even.

12. (Komal A277) Let p be a prime number and H_1 be a p-gon. Construct the sequence of polygons $H_1, H_2, \cdots, H_p$ as follows: once H_k is constructed, reflect each vertex by the k-th vertex clockwise from it. Show that H_1 and H_p are similar.

A Equidistribution

You might know the fact that the fractional parts of $n\sqrt{2}$ are dense mod 1. In fact, they must be "uniformly distributed" - a way to measure this is to look at an interval $(a,b) \subset [0,1)$ and see what proportion of the fractional parts of $n\sqrt{2}$ lie in (a,b). If this always approaches $b-a$, we also say that the fractional parts of $n\sqrt{2}$ are **equidistributed** mod 1.

How do we figure out if a sequence is equidistributed?

Fact 12 (Weyl's criterion)

A sequence $a_1, a_2, \cdots$ is equidistributed mod 1 if and only if

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i a_n} = 0.$$

One can think of this as a case of the more general statement that

$$\frac{1}{N}\sum_{n=1}^{N} f(a_n) \to \int_0^1 f(x)dx.$$

for bounded functions f - we're saying that it's sufficient (and equivalent) to check this for (1) $f \in \{\mathbb{I}_{(a,b)}\}$ or (2) $f(x) \in \{e^{2\pi i k x}\}_{k\in\mathbb{Z}}$.

This feels like some kind of Fourier transform, doesn't it?

A cool application of this fact is

Fact 13 (van der Corput's difference theorem)

If $\{a_{n+h} - a_n\}$ is equidistributed mod 1 for all positive integers h, then $\{a_n\}$ is equidistributed mod 1.

which proceeds by moving to the exponential sum and doing some bounding there. As a consequence, this tells us that all polynomials with irrational leading coefficients are equidistributed mod 1!

B Counting solutions mod p

By pretending that the primitive root g is a $(p-1)$-th root of unity, we get (for $k > 0$):

$$\sum_{x\in\mathbb{F}_p} x^k \equiv -\mathbb{I}_{(p-1)|k} \pmod p.$$

As we saw earlier on in "advanced usage", these things stack very nicely multiplicatively. For example:

$$\sum_{x,y\in\mathbb{F}_p} x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m} \equiv (-1)^m \cdot \mathbb{I}_{(p-1)|k_i, i=1,\ldots,m} \pmod p$$

This can be used to prove a very cute theorem:

Fact 14 (Chevalley's theorem)

Suppose you have a system of polynomial equations mod p such that there are more variables than the sum of the total degree across each coefficient. Then, if it has a trivial solution (i.e. all 0s), it also has at least one non-trivial solution.

Proof. Suppose our system of equations is $f_1 = f_2 = ... = f_m = 0$ over variables $x_1, ..., x_m$. Then, note that

$$1 - f(x)^{p-1} \equiv \mathbb{I}_{f(x)\equiv 0 \pmod p} \pmod p$$

Thus, the following sum counts the solutions mod p:

$$\sum_{x_1,\dots,x_n} (1 - f_1(x_1, ..., x_n)^{p-1}) \cdots (1 - f_m(x_1, ..., x_n)^{p-1})$$

but clearly it has degree less than $n(p-1)$, so the sum on each monomial vanishes. Hence, the number of solutions is a multiple of p.

C Characters on finite abelian groups

Recall the fundamental fact that we saw above:

$$\sum_{k=1}^{n} e^{2\pi i k x/n} = 0, \quad \text{if } x \in \mathbb{Z}_{\neq 0}.$$

We also saw that we can multiply these together:

$$\sum_{k=1}^{n} \sum_{\ell=1}^{m} \exp\left(2\pi i \left(\frac{kx}{n} + \frac{\ell y}{m}\right)\right) = 0, \quad \text{if } (x, y) \neq (0, 0).$$

In fact, we're able to abstract what's special here and use it for any finite abelian group: we just need the group operation "+" on G to commute with multiplication in $\mathbb{C}$, i.e. for a map $\psi : G \to \mathbb{C}^*$ to satisfy

$$\psi(a + b) = \psi(a) \cdot \psi(b).$$

(The reason we use $\mathbb{C}^*$ instead of $\mathbb{C}$ is because if any value is zero, then ψ is identically 0.) Such a ψ is called a **character**, and we also say that ψ is **trivial** if $\psi \equiv 1$ and **nontrivial** otherwise.

A new example of a character is the Legendre symbol, which tells you if a residue is a perfect square or not. This ends up being a character of the multiplicative group $\mathbb{F}_p^\times$, where the operation is multiplication instead of addition:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue} \\ -1 & \text{if } a \text{ is a quadratic nonresidue} \\ 0 & \text{if } a \equiv 0 \pmod p \end{cases}$$

The crucial fact is that we have **orthogonality** for characters: for characters χ and χ', define

$$\langle \chi, \chi' \rangle := \frac{1}{|G|} \sum_{g\in G} \chi(g)\overline{\chi'(g)} = \mathbb{I}_{\chi=\chi'}.$$

Geometrically speaking, this is saying that the characters form an orthonormal basis (using this particular inner product). If we substitute $\chi = \mathbb{1}$, we have the usual

$$\sum_{g\in G} \chi(g) = \begin{cases} |G| & \text{if } \chi \text{ is trivial} \\ 0 & \text{otherwise.} \end{cases}$$

D Gauss/Jacobi sums

When I was taking a field theory class I had this really cool problem:

Example 15

Show that for odd primes p,

$$\left|\sum_{a\in\mathbb{F}_p} e^{2\pi i a^2/p}\right| = \sqrt{p}$$

See if you can solve it! This is the simplest case of what's called a **Gauss sum**, and much more is known - for example, the sum is exactly

$$\begin{cases}\sqrt{p} & \text{if } p\equiv 1 \pmod 4;\\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4).\end{cases}$$

What's interesting is that we can rewrite this slightly in terms of the Legendre symbol:

$$\sum_{a\in\mathbb{F}_p} e^{2\pi i a^2/p} = \sum_{a\in\mathbb{F}_p}\left(1+\left(\frac{a}{p}\right)\right)e^{2\pi i a/p} = \sum_{a\in\mathbb{F}_p}\left(\frac{a}{p}\right)e^{2\pi i a/p}.$$

This forms the general definition of a Gauss sum: for a character χ of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, the Gauss sum is

$$G(\chi) = \sum_{a\in\mathbb{Z}/n\mathbb{Z}} \chi(a)e^{2\pi i a/n}.$$

and we know a couple of properties:

- $|G(\chi)| = \sqrt{n}$ if χ is primitive (i.e. not induced by a character of a smaller modulus).
- Let's also define the **Jacobi sum** $J(\chi,\psi) = \sum_a \chi(a)\psi(1-a)$.
- $J(\chi,\psi) = \frac{G(\chi)G(\psi)}{G(\chi\psi)}$.
- If χ is the Legendre symbol, then $J(\chi,\chi) = (-1)^{(p+1)/2}$.
- (Weil bounds; see this link) In the prime setting, for a nonzero polynomial P which is not the scalar multiple of a d-th power (where d is the order of χ), we have

$$\left|\sum_{a\in\mathbb{F}_p}\chi(P(a))\right| \le d\sqrt{p}.$$

The Gauss sum can also be used to prove the quadratic reciprocity law, but for brevity I won't go into it here.

E Fourier expansions

A Fourier expansion is a way to represent a function as known periodic functions. In an engineering textbook, you might see

$$f(x) = a_0 + \sum_{n=1}^{\infty}(a_n\cos(2\pi nx) + b_n\sin(2\pi nx))$$

or if you prefer the exponential basis:

$$f(x) = \sum_{n\in\mathbb{Z}} c_n e^{2\pi i n x}$$

where the c_n are the Fourier coefficients.

There is some theory (google "Schwartz functions") around when these coefficients exist and define a convergent sum, but for the kind of heuristics we're doing it's fine to assume that it exists.

We give one example where this intuition is useful:

Example 16

Prove that:

$$\sum_{j,k=1}^{n} \frac{a_j a_k}{1+|j-k|} \geq 0$$

Solution. The idea here is that such a sum can be "decomposed" into positive sums like

$$\sum_{j,k=1}^{n} a_j a_k \cos((j-k)x) = \sum_{j,k=1}^{n} a_j a_k e^{2\pi i(j-k)x} = \left| \sum_{j=1}^{n} a_j e^{2\pi ijx} \right|^2.$$

So it would be nice if there was a function $k(x)$ (sometimes called a "kernel") such that

$$\frac{1}{1+|n|} = \int k(x) e^{2\pi inx} dx$$

where $k(x) \geq 0$. A free way to get a k that satisfies the above (but not necessarily non-negative) is to consider

$$k_0(x) = \sum_{n\in\mathbb{Z}} \frac{1}{1+|n|} e^{2\pi inx}$$

which we recognize as the Fourier transform of $\frac{1}{1+|n|}$. This is a function on "$\mathbb{R}$ mod 1". Now, this can be reversed by the inverse Fourier transform:

$$\frac{1}{1+|n|} = \int_0^1 k_0(x) e^{-2\pi inx} dx$$

So it remains to check that this kernel is indeed non-negative. Well, we use the trick of representing the fraction as an integral:

$$\begin{aligned} k_0(x) &= \sum_{n\in\mathbb{Z}} \frac{1}{1+|n|} e^{2\pi inx} \\ &= \int_0^1 \sum_{n\in\mathbb{Z}} e^{2\pi inx} r^{|n|} dr \\ &= \int_0^1 \frac{1-r^2}{1-2r\cos(2\pi x)+r^2} \geq 0. \end{aligned}$$

□

F Fourier for Boolean algebras

In a different land there is another kind of sum that gives an indicator function:

$$\sum_{J\subseteq I} (-1)^{|J|} = \mathbb{I}_{|I|=0}$$

and its "relative" cousin:

$$\sum_{I'\subseteq J\subseteq I} (-1)^{|J|} = \mathbb{I}_{I=I'}.$$

Here's one implication: suppose I have one number per subset $\{a_I\}_{I\subseteq[n]}$, and we had

$$A_I = \sum_{J\subseteq I} a_J.$$

Then, we can recover a_I from A_I using

$$\begin{aligned}\sum_{J\subseteq I}(-1)^{|I|+|J|}A_J &= \sum_{J\subseteq I}(-1)^{|I|+|J|}\sum_{K\subseteq J}a_K\\ &= \sum_{K\subseteq J\subseteq I}(-1)^{|I|-|J|}a_K\\ &= \sum_{K\subseteq I}a_K\mathbb{I}_{K=I}\\ &= a_I\end{aligned}$$

You might realize that this proves the Principle of Inclusion-Exclusion.