Divided Differences

Kada Williams

June 15, 2017

This article, aimed at beginners, investigates a theory of algebraic expressions, ultimately explaining the celebrated Combinatorial Nullstellensatz. While this topic is very loosely related to Olympiads, I hope it will be a lot of fun. [1]

Contents

[1] For the fancy Latex, I used Evan Chen's evan.sty, from his website `http://web.evanchen.cc`.

§1 Foreword

My not-so-secret goal with writing this article is to give you an experience

- that math which seems *very advanced* is at times actually *very easy*, and
- how us humans can build up complex and deep ideas *if* we keep looking at what we know from a distance.

In other words, we can think about complicated things if we can understand them in simple terms:

1. we can *rephrase* what we want to prove more compactly,
2. we can *visualize* objects (that's what our brains evolved for!),
3. we can use *notation/language* to think about complex processes in simple terms (e.g. "if I do X, then Y happens except if V; if I also can do U, then V doesn't happen, so let's do X with U" is how 20-page proofs are created).

Therefore, even if Divided Differences had absolutely nothing to do with anything you want to get done, it may be worth reading this article to learn about *how* ideas can build onto each other.

§2 Difference sequences

§2.1 Let's Take Differences!

Let's start with a sequence $a_0, a_1, a_2, \ldots$, and compose the differences of the neighboring terms, generating the sequence $b_n = a_{n+1} - a_n$. For example,

$$\begin{array}{ccccccccccccccc}
0 & & 1 & & 4 & & 9 & & 16 & & 25 & & 36 & & \ldots \\ \hline
& 1 & & 3 & & 5 & & 7 & & 9 & & 11 & & \ldots &
\end{array}$$

Starting from a sequence $(a_n)_{n\geq 0}$, we can generate sequences (b_n), (c_n), $\ldots$ with $b_n = a_{n+1} - a_n$, $c_n = b_{n+1} - b_n$, $\ldots$, arranging them like this:

$$\begin{array}{ccccccccccc}
a_0 & & a_1 & & a_2 & & a_3 & & a_4 & & \ldots \\ \hline
& b_0 & & b_1 & & b_2 & & b_3 & & \ldots & \\ \hline
& & c_0 & & c_1 & & c_2 & & \ldots & & \\ \hline
& & & \ldots & & \ldots & & \ldots & & &
\end{array}$$

Example 2.1

Calculate the first few terms of the difference sequences when $a_n = n$, $a_n = n^2$, $a_n = n^3$, and $a_n = n^4$.

Here's the array for $a_n = n^3$:

$$\begin{array}{ccccccccccccc}
0 & & 1 & & 8 & & 27 & & 64 & & 125 & & \ldots \\ \hline
& 1 & & 7 & & 19 & & 37 & & 61 & & \ldots & \\ \hline
& & 6 & & 12 & & 18 & & 24 & & \ldots & & \\ \hline
& & & 6 & & 6 & & 6 & & \ldots & & & \\ \hline
& & & & 0 & & 0 & & 0 & & \ldots & &
\end{array}$$

Problem 2.2. Let k be a positive integer. What do you think will happen when $a_n = n^k$?

Here's another question to think about:

Example 2.3

Here's the array for $a_n = n^3 + 5n$:

0		6		18		42		84		150		...
	6		12		24		42		66		...	
		6		12		18		24		...		
			6		6		6		...			
				0		0		0		...		

Do you notice anything?

Try to come up with conjectures (*observations*) and try to imagine possibly vague reasons for why your conjectures should be true (*intuition*). We will later find memorable ways to make sense of that intuition, and concoct proofs out of them.

Observations:

- Eventually, we will end up with a row full of 0's, and before that, there is a constant sequence.
- Let $a_n = n^k$. This constant is actually $k!$.
- If the first row is Row 0, the second is Row 1, and so on, then Row k will be $k!, k!, \dots$ and Row $k+1$ will be $0, 0, \dots$.
- We can get the array for $a_n = n^3 + 5n$ by just adding [the array for $a_n = n^3$] and [$5\times$ the array for $a_n = n$].

Intuitively, the experience is that taking differences first creates some chaos, but then taking differences a few more times "eats up" the confusion. This makes sense, because in general, when we take differences, often some terms vanish, for example

$$(n+1)^3 - n^3 = (n^3 + 3n^2 + 3n + 1) - n^3 = 3n^2 + 3n + 1.$$

Observe how when we got $b_n = 3n^2 + 3n + 1$ from $a_n = n^3$, the formula for the terms in b_n ended up having so-called *degree* 2, because the n^3 terms *cancelled*.

§2.2 Formal Series and Polynomials

What did we mean by *degree* before? We said that n^3 has degree 3, but $3n^2 + 3n + 1$ has degree 2.

The concept *degree* doesn't have to do with the actual value of our expressions, rather with the expressions themselves. This is just like how in grammar, there's a difference between the meaning of words (what we think of when reading a word) and the words themselves (the set of characters we write down).

This section serves to solidify the reader's understanding of polynomial expressions while clarifying this distinction.

Consider a so-called polynomial expression $f(n)$, such as $f(n) = n^3$ or $f(n) = 3n^2 + 3n + 1$. The **substitution value** of the polynomial is what value it takes at a certain value at n, such as $f(5)$ or $f(42)$. When we rather talk about the symbols themselves, i.e. the expression "$3n^2 + 3n + 1$", we talk about polynomials **formally**.

Consider some real numbers $a_0, a_1, \dots$, and look at the *formal* sum

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k + \dots.$$

If for some k, $a_{k+1} = a_{k+2} = \cdots = 0$, then we call this expression a polynomial. In general, this sum could be infinite as well – then, we call it a formal series. This way, each formal series $f(x)$ corresponds to a sequence $(a_0, a_1, \dots)$ and vice versa.

We can now define addition, subtraction and multiplication on formal sums[2].

Let $f(x) = a_0 + a_1 x + \dots$ and $g(x) = b_0 + b_1 x + \dots$. Then $f(x) \pm g(x)$ is the formal series corresponding to the sequence

$$(a_0 \pm b_0, a_1 \pm b_1, \dots, a_k \pm b_k, \dots).$$

[2] In abstract algebra, a set $R(+,\cdot)$ with 'units' like $0, 1$, addition, additive inverses ($x \mapsto -x$), and multiplication which does $a \cdot (b + c) = a \cdot b + a \cdot c$ is called a *commutative ring*.

Example 2.4

Let $f(x) = x^2 + x + 1$ and $g(x) = x + 3$. Then

$$f(x) - 3g(x) = x^2 - 2x - 8.$$

What is $f(x) \cdot g(x)$? No, it isn't $(a_0b_0) + (a_1b_1)x + \dots$, for example. We want to define multiplication in a way that if we *substitute* any value for x and evaluate the sums (pretend that we can do infinite addition), the multiplication still remains true[3]. This way, $f(x) \cdot g(x)$ becomes the formal series corresponding to the sequence

$$\Big(a_0b_0, (a_0b_1 + a_1b_0), (a_0b_2 + a_1b_1 + a_2b_0), \dots, (a_0b_k + a_1b_{k-1} + \dots + a_kb_0), \dots\Big).$$

Example 2.5

We have

$$\begin{aligned}(4 - x + x^2 + 0x^3 + 0x^4 + \dots)(3 + 2x + x^2 + 0x^3 + 0x^4 + \dots) &= \\ = 12 + 8x &+ 4x^2 \\ -3x &- 2x^2 - x^3 \\ &+ 3x^2 + 2x^3 + x^4 \\ = 12 + 5x &+ 5x^2 + x^3 + x^4.\end{aligned}$$

Recall that polynomials are the formal series

$$P(x) = a_0 + a_1x + \dots + a_kx^k + \dots$$

where the *coefficients* $a_0, a_1, \dots$ are eventually all 0. In particular, if $a_d \neq 0$ but $a_{d+1} = a_{d+2} = \dots = 0$, we say that d is the *degree* of P, and that a_d is the *leading coefficient*. On and in the exceptional case $a_0 = a_1 = \dots = 0$, we say P is the *zero polynomial*, and define its degree as "$-\infty$".

We can perform $+$ and $\cdot$ on polynomials, too. The sum and product of polynomials remains a polynomial.

Example 2.6

What does addition and multiplication do to a polynomial's degree?

Also, note that we could have defined polynomials without talking about formal series had I felt like it.

We can also talk about powers of polynomials: $f(x)^2 = f(x) \cdot f(x)$, $f(x)^3 = f(x)^2 \cdot f(x)$, and so on. The polynomial $f(x+1)$ comes from $f(x) = \dots + a_kx^k + \dots$ by fully expanding all the terms $a_k(x+1)^k$ using the Binomial Theorem:

[3] Higher math would say that the evaluation map from the ring of formal power series to the reals defined by $f(x) \mapsto f(r)$ should be a (ring) *homomorphism*. (Well, OK, that's just wrong – e.g. $1 + 1 + 1 + \dots$ does not exist –, but Calculus does prove that there is a subring of formal series where $f(r)$ exists.) Think about why it could be worth talking about math like this.

Theorem 2.7

Consider the Pascal triangle. Note how its n-th row can be encoded by the polynomial

$$\binom{n}{0} + \binom{n}{1}x^1 + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Since the Pascal triangle is an addition table, i.e. $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$, when we formally multiply this polynomial by $(1+x)$, we get the polynomial encoding the $(n+1)$-th row. This means that the polynomial encoding row 1 is $1+x$, the one encoding row 2 is $(1+x)^2$, and so on:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x^1 + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

We call this idea the Binomial Theorem.

One more thing: from now on, I'll use $\sum$ (sum) notation. So for example, a polynomial or formal power series could be called $f(x) = \sum a_k x^k$. Additionally, if I wanted to specify that I only wish to add terms with $k = 0, 1, \ldots, n$, then I'd write $f(x) = \sum_{k=0}^{n} a_k x^k$. Similarly, I can do things like

$$\sum_{j=0}^{n} (-1)^j x^{2j} = 1 - x^2 + x^4 - x^6 + \cdots + (-1)^n x^{2n}.$$

Now let's return to our observations about finite differences and prove them!

§2.3 More on Finite Differences

Remember how we defined $b_n = a_{n+1} - a_n$ from (a_n)? Now let $f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0$ be a polynomial, and consider $a_n = f(n)$. Define

$$f_1(x) = f(x+1) - f(x), \quad \ldots, \quad f_{m+1}(x) = f_m(x+1) - f_m(x).$$

We already know that the degree of these polynomials decreases, i.e. $\deg f > \deg f_1 > \deg f_2 > \ldots$[4]. We can actually say more.

Theorem 2.8

Using the Binomial Theorem and considering the array generated by $a_n = n^k$ and by $a_n = \alpha_{k-1}n^{k-1} + \cdots + \alpha_0$, prove that $\deg f_1 = \deg f - 1$. Next, prove that $\deg f_m = \deg f - m$ $(2 \le m \le k)$.

In fact, if the leading term of $f(x)$ is x^k, then the leading term of $f_1(x)$ is kx^{k-1}, the leading term of $f_2(x)$ is $k(k-1)x^{k-2}$, and so on. By the time we get to $f_{k+1}(x)$, every term will have vanished, so $f_{k+1}(x)$ is the zero polynomial. Similarly, $f_k(x)$ is a constant, and it is equal to its leading term

$$k(k-1)(k-2) \cdot \ldots \cdot 1 = k!\,.$$

[4] Recall how we made the zero polynomial have degree $-\infty$; just pretend that $-\infty > -\infty$.

§2.4 Some problems

Problem 2.9. Let $f(x)$ be a polynomial, and suppose that $f_{k+1}(x) \equiv 0$, i.e. f_{k+1} is formally equal to the zero polynomial. What can we say about $f(x)$?

Problem 2.10. Invoke the Pascal triangle to find that actually,

$$f_\ell(x) = f(x+\ell) - \binom{\ell}{1} f(x+\ell-1) \pm \cdots + (-1)^\ell f(x) = \sum_{j=0}^{\ell} (-1)^{n-j} \binom{n}{j} f(x+j).$$

Problem 2.11. Let $a_n = 2^n$. What are the difference sequences? What about $a_n = \lambda^n$?

Problem 2.12. Define the Fibonacci sequence by $F_0 = F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ $(n \geq 1)$. For $m \leq n$, simplify

$$\sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} F_{n+j}.$$

Problem 2.13. Let p be an odd prime number. Prove that $F_{n+p} - F_n - F_{n-p}$ is a multiple of p.

Problem 2.14. Let $f(x)$ be any polynomial with integer coefficients, and let p be a prime number. Prove that every coefficient of $f_m(x)$ is divisible by p if $m \geq p$.

Problem 2.15. The difference operator Δ_h creates new functions from functions: from $f(x)$, it creates $\Delta_h f(x) = f(x+h) - f(x)$. Prove the following:

(a) If Δ_h^n is Δ_h applied n times,

$$\Delta_h^n f(x) = \sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} f(x+jh).$$

(b) Difference operators *commute*, i.e. $\Delta_a(\Delta_b f(x)) = \Delta_b(\Delta_a f(x))$, and we have the *product rule*

$$\Delta_h(f(x)g(x)) = f(x+h) \cdot \Delta_h g(x) + g(x) \cdot \Delta_h f(x).$$

(c) If $f(x)$ is a polynomial of degree $d > 0$, then $\Delta_h f(x)$ is a polynomial of degree $d-1$.

Problem 2.16. Research project: suppose that (a_n) is periodic with period m. Then we can encode it as $P(x) = a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$. Look at the difference sequences of (a_n) modulo 2, or maybe modulo some odd prime p. What's the pattern? Prove stuff.

§3 Divided Differences

§3.1 Introduction and Motivation

Consider the following identities:

$$\begin{aligned}(x+1)^2 - x^2 &= 2x+1\\ (x+a)^2 - x^2 &= 2ax + a^2\\ (x+a)^3 - x^3 &= 3ax^2 + 3a^2x + a^3\end{aligned}$$

which are essentially ugly, and also consider the identities

$$\begin{aligned}y^2 - x^2 &= (y-x)(y+x)\\ y^3 - x^3 &= (y-x)(y^2+yx+x^2)\\ \frac{1}{y} - \frac{1}{x} &= (y-x)\left(-\frac{1}{xy}\right)\end{aligned}$$

which are fairly nice.

These tell us, for example, that for polynomials P, the expression $P(x+a) - P(x)$ is messier to work with than $\frac{P(y)-P(x)}{y-x}$, in particular because

$$\frac{y^k - x^k}{y-x} = x^{k-1}y + x^{k-2}y^2 + \cdots + y^{k-1}$$

is a polynomial expression – not in 1 variable, but in 2 variables, instead.[5]

Just as how a polynomial in one variable is an expression of the form $\sum a_k x^k$, we can talk about *multivariate* polynomials such as $y^2 + x$ and $x_1 + x_2 - 2x_3^5$. A polynomial in variables $x_1, \dots, x_n$ is defined as an expression which is a finite sum of so-called *monomials*, i.e. a finite sum of expressions of the form $C_{d_1,d_2,\dots,d_n} x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$. The *degree* of such a monomial is $d_0 + d_1 + \cdots + d_n$, and the degree of a multivariate polynomial is the maximal degree of its monomials.[6]

Example 3.1

We can extend this to 3 variables:

$$\begin{aligned}\frac{y^3 - x^3}{y-x} &= y^2 + yx + x^2,\\ \frac{\frac{y^3-x^3}{y-x} - \frac{z^3-x^3}{z-x}}{y-z} &= \frac{(y^2+yx+x^2) - (z^2+zx+x^2)}{y-z}\\ &= \frac{y^2-z^2}{y-z} + \frac{x(y-z)}{y-z} + \frac{x^2(1-1)}{y-z} = x+y+z.\end{aligned}$$

§3.2 Definition

Start from a function $f(x)$, and create the function $g(x,y) = \frac{f(x)-f(y)}{x-y}$ $(x \neq y)$. Now repeat this step by constructing

$$h(x,y,z) = \frac{g(x,y) - g(x,z)}{y-z} \qquad (y \neq z),$$

[5] Strictly speaking, we didn't define *division* by polynomials, so here it is: if $p(x) = q(x)r(x)$ and $q(x) \not\equiv 0$, then we define $r(x) = \frac{p(x)}{q(x)}$.

[6] In a fashion akin to our skirmish with formal series, one can define the sum and product of multivariate polynomials, but I omit this, because it is intuitively obvious.

which is just doing the same thing, as if x weren't even there.

Example 3.2
Calculate that

$$h(x,y,z) = \frac{f(x)}{(x-y)(x-z)} + \frac{f(y)}{(y-x)(y-z)} + \frac{f(z)}{(z-x)(z-y)}.$$

Starting from a function $f(x)$, we can extend this process to $n+1$ variables $x_0, x_1, \dots, x_n$ by defining

$$f_1(x_0, x_1) := \frac{f(x_0) - f(x_1)}{x_0 - x_1},$$
$$f_m(x_0, x_1, \dots, x_m) := \frac{f_{m-1}(x_0, \dots, x_{m-2}, x_{m-1}) - f_{m-1}(x_0, \dots, x_{m-2}, x_m)}{x_{m-1} - x_m}.$$

In this case, we call

$$f[x_0, x_1, \dots, x_n] := f_n(x_0, \dots, x_n)$$

the n-th order **divided difference** of f.

Problem 3.3. Prove that

$$f[x_0, x_1, \dots, x_n] = \sum_{j=0}^{n} \frac{f(x_j)}{(x_j - x_0)\dots(x_j - x_{j-1})(x_j - x_{j+1})\dots(x_j - x_n)}.$$

In particular, note that $f[x_0, x_1, \dots, x_n]$ is *symmetric*: it doesn't depend on the order of $x_0, x_1, \dots, x_n$.

Problem 3.4. Prove that if $f(x)$ is a polynomial of degree $N \geq n$, then $f[x_0, x_1, \dots, x_n]$ is a multivariate polynomial of degree $N - n$. [7]

Problem 3.5. Let x, y, z be integers. Prove that

$$\frac{x^4}{(x-y)(x-z)} + \frac{y^4}{(y-x)(y-z)} + \frac{z^4}{(z-x)(z-y)}$$

is also an integer.

Problem 3.6. Prove that in fact, if $f(x) = x^N$, then for $n < N$, [8]

$$f[x_0, x_1, \dots, x_n] = \sum_{\substack{d_0+d_1+\dots+d_m=N-n \\ d_0,d_1,\dots,d_m \geq 0}} x_0^{d_0} x_1^{d_1} \dots x_n^{d_n}.$$

Problem 3.7. Prove that if $f(x)$ is a polynomial of degree N, then $f[x_0, x_1, \dots, x_N]$ is a constant equal to the leading coefficient of f, and that $f[x_0, x_1, \dots, x_n]$ is the zero polynomial if $n > N$.

[7] Unrelated but interesting: Lexicographical order.

[8] This big ugly sum means that we add up the monomial $x_0^{d_0} x_1^{d_1} \dots x_n^{d_n}$ for any possible $(n+1)$-tuple of nonnegative integers $d_0, \dots, d_n$ whose sum is $N - n$.

§3.3 Application: Roots of Multivariate Polynomials

Let $K = \mathbb{R}$, and call $K[x]$ the set of polynomials with coefficients in K. [9]

Theorem 3.8

If $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in K[x]$, then f has at most d distinct roots, i.e. there are at most d distinct numbers $x \in K$ for which $f(x) = 0$.

Proof. Note that

$$f[x_0, x_1, \ldots, x_d] = \sum_{j=0}^{d} \frac{f(x_j)}{(x_j - x_0)\ldots(x_j - x_{j-1})(x_j - x_{j+1})\ldots(x_j - x_d)} \equiv 1$$

due to Problem 3.7. But if $x_0, x_1, \ldots, x_d \in K$ are pairwise different, and $f(x_j) = 0$ for each $j = 0, 1, \ldots, d$, then $f[x_0, x_1, \ldots, x_d] = 0$. Since $0 \neq 1$, this shows that f cannot have more than d distinct roots. $\square$

Now bear with me while we generalize this:

Theorem 3.9

Let $f(x, y)$ be a 2-variable polynomial with coefficients from K. Let its degree be d, in which case it must have some monomial $Cx^k y^\ell$ with $C \neq 0$ and $k + \ell = d$.

Then there cannot be sets $S, T \subset K$ with $|S| = k + 1$ and $|T| = \ell + 1$ such that for any $x \in S$ and $y \in T$, $f(x, y) = 0$.

Proof. Recall how when defining divided differences, we took some function $g(Y, X_0, X_1, \ldots)$ and created the new function $\frac{g(Y,X_0,X_1,\ldots)-g(Z,X_0,X_1,\ldots)}{Y-Z}$. This involved caring about one variable and leaving the rest alone.

Since $f(x, y)$ has two variables, we're going to do the same process as before twice. First, we leave y alone, and repeat taking differences, resulting in the function

$$g(x_0, x_1, \ldots, x_k, y) = \sum_{i=0}^{k} \underbrace{\frac{1}{(x_i - x_0)\ldots(x_i - x_k)}}_{=:A_i} \cdot f(x_i, y).$$

Second, we leave $x_0, x_1, \ldots, x_k$ alone, and repeat taking differences, which yields

$$\begin{aligned} h(x_0, x_1, \ldots, x_k, y_0, y_1, \ldots, y_\ell) &= \sum_{j=0}^{\ell} \underbrace{\frac{1}{(y_j - y_0)\ldots(y_j - y_\ell)}}_{=:B_j} g(x_0, \ldots, x_k, y_j) \\ &= \sum_{j=0}^{\ell} B_j(y_0, \ldots, y_\ell) \left(\sum_{i=0}^{k} A_i(x_0, \ldots, x_k) f(x_i, y_j) \right). \end{aligned}$$

Note that $f(x, y)$ is the sum of monomials of the form $Ax^\kappa y^\lambda$. Just like how with finite differences, the array belonging to $(a_n + a'_n)$ was the sum of the array belonging to (a_n)

[9] Everything here works for any field K. For example, taking $K = \mathbb{F}_p$ in Theorem 3.8 gives Lagrange's theorem.

and the array belonging to (a'_n), here too, the function $h(x_0, \ldots, y_\ell)$ generated by $f(x, y)$ is just the sum of the h's we get when applying the same process to each monomial $Ax^\kappa y^\lambda$ in the expansion of $f(x, y)$.

Now look at what happens if we replace $f(x, y)$ by $x^\kappa y^\lambda$ in the definition of h. Then h factors!

$$\sum_{j=0}^{\ell} B_j \left(\sum_{i=0}^{k} A_i x_i^\kappa y_j^\lambda \right) = \left(\sum_{j=0}^{\ell} B_j y_j^\lambda \right) \cdot \left(\sum_{i=0}^{k} A_i x_i^\kappa \right).$$

Here, the first factor is the ℓ-th order divided difference of y^λ, while the second is the k-th order divided difference of x^κ. Hence, if $[\kappa < k$ or $\lambda < \ell]$, then this product is $\equiv 0$, and if $[\kappa = k$ and $\lambda = \ell]$, then this product is $1 \cdot 1 = 1$.

Returning to f and h, we thus have $h(x_0, \ldots, y_\ell) \equiv C \neq 0$. However, if we could have some $S = \{x_0, \ldots, x_k\}$ and $T = \{y_0, \ldots, y_\ell\}$ with $f(x_i, y_j) = 0$ $(x_i \in S, y_j \in T)$, then just as in Theorem 3.8, we'd get $h(x_0, \ldots, y_\ell) = 0$, a contradiction. $\square$

This method repeats itself in a slightly different form in the key lemma for problem 6 of IMO 2007:

Theorem 3.10

Suppose $P(x, y, z)$ is a polynomial which satisfies $P(x, y, z) = 0$ if $x, y, z \in \{0, 1, \ldots, n\}$ and $(x, y, z) \neq (0, 0, 0)$. If $P(0, 0, 0) \neq 0$, then $\deg P \geq 3n$.

Proof. We do the same thing, except now $\{x_0, \ldots, x_n\} = \{0, 1, \ldots, n\}$, so mere differences will suffice, actually. To any polynomial $Q(x, y, z)$, assign the real number

$$h_Q := \sum_{x=0}^{n} (-1)^{n-x} \binom{n}{x} \left(\sum_{y=0}^{n} (-1)^{n-y} \binom{n}{y} \left(\sum_{z=0}^{n} (-1)^{n-z} \binom{n}{z} Q(x, y, z) \right) \right).$$

Again, if $Q(x, y, z) = Ax^\alpha y^\beta z^\gamma$, then h_Q factors into the finite differences of $x^\alpha, y^\beta, z^\gamma$. Hence, if one of α, β, γ is less than n, then $h_Q = 0$.

When we split some Q into a sum of polynomials, h_Q will be the sum of the corresponding h's. This means that $\deg Q \leq 3n - 1$ implies $h_Q = 0$, because then Q only contains monomials $Ax^\alpha y^\beta z^\gamma$ where one of the exponents is $< n$.

Since $h_P = (-1)^n \binom{n}{0} (-1)^n \binom{n}{0} (-1)^n \binom{n}{0} P(0, 0, 0) \neq 0$, this proves that $\deg P \leq 3n - 1$ is impossible, so $\deg P \geq 3n$. $\square$

The unusual thing here was that we didn't need to evaluate h_Q for $x^n y^n z^n$. That made the proof a bit simpler. If we wanted to make the proof look more like Theorem 3.9, we should have instead taken

$$P^*(x, y, z) = P(x, y, z) - k\,[(x-1)\ldots(x-n)(y-1)\ldots(y-n)(z-1)\ldots(z-n)]$$

where $k \neq 0$ is chosen such that $P^*(x, y, z) = 0$ for any $x, y, z \in \{0, 1, \ldots, n\}$. Then a version of Theorem 3.9 would have proven that $P^*(x, y, z)$ cannot have degree $3n$ and a monomial $Cx^n y^n z^n$ with $C \neq 0$ at the same time, which leads to a contradiction.

The general version of Theorem 3.9 is called the Combinatorial Nullstellensatz:

Theorem 3.11

Let $f(x_1, x_2, \ldots, x_n)$ be a polynomial with coefficients from K. Let $Cx_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ be a monomial appearing in f which has maximal degree ($C \neq 0$). Then we cannot have sets $S_1, S_2, \ldots, S_n$ with $|S_i| = d_i + 1$ for which

$$f(x_1, x_2, \ldots, x_n) = 0 \qquad \text{whenever} \qquad x_1 \in S_1, x_2 \in S_2, \ldots, x_n \in S_n.$$

Proof. The same as Theorem 3.9. Repeatedly take divided differences with respect to each variable of $Q(x_1, x_2, \ldots, x_n)$, getting a polynomial h_Q in $(d_1+1)+(d_2+1)+\cdots+(d_n+1)$ variables. On one hand, the divided difference of a monomial factors, from which we can compute that $h_f \equiv C \neq 0$. On the other hand, if such sets $S_1, S_2, \ldots, S_n$ did exist, then plugging in the elements of the sets into h_f would make $h_f = 0$, contradiction. $\square$

§4 More Problems

§4.1 Difference Sequences

Problem 4.1. Define $a_n = f(n)$, where

$$f(x) = \binom{x}{k} := \frac{x(x-1)\ldots(x-k+1)}{k!}.$$

(a) Find the difference sequences of a_n.

(b) Prove that every polynomial can be expressed in the form $c_k\binom{x}{k}+c_{k-1}\binom{x}{k-1}+\cdots+c_0$ for some reals $c_k, c_{k-1}, \ldots, c_0$. [10]

(c) Prove that $f(x)$ takes on integer values whenever x is an integer if and only if $c_k, c_{k-1}, \ldots, c_0$ are all integers.

(d) Give another proof that when starting from $f(x) = x^k$, we'll have $f_k(x) = k!$.

Problem 4.2. Let $\Delta_h f(x) = f(x+h) - f(x)$ be the difference operator. Let $s_2(n)$ denote the sum of digits of n when written in binary[11]. After writing down a few special cases, prove that

$$\Delta_{2^{k-1}}\Delta_{2^{k-2}}\ldots\Delta_1 f(x) = \sum_{j=0}^{2^k-1}(-1)^{s_2(j)} f(x+(2^k-j)).$$

Problem 4.3. Fix a positive integer k. Prove that for some N, we can partition the numbers $1^k, 2^k, \ldots, N^k$ into two groups of equal sums.

Problem 4.4. Let $a \geq 3$, and let P be a polynomial whose degree is $< n$. Prove that we cannot have

$$\delta_k := a^k - P(k) \in (-1; 1)$$

for each $k = 0, 1, \ldots, n$.

[10] Higher math would say that $\{1, \binom{x}{1}, \binom{x}{2}, \ldots\}$ forms a basis of the vector space $\mathbb{R}[x]$ over $\mathbb{R}$.
[11] See the Thue-Morse sequence.

Problem 4.5. If you know complex numbers, let $\varepsilon = \operatorname{cis} \frac{2\pi\ell}{m}$ for some $\ell \in \{0, 1, \ldots, m-1\}$, and define the operator D_h by

$$D_h f(x) = f(x) + \varepsilon f(x+h) + \varepsilon^2 f(x+2h) + \cdots + \varepsilon^{m-1} f(x+(m-1)h).$$

Using D_h, prove that for some N, we can partition the numbers $1^k, 2^k, \ldots, N^k$ into m groups of equal sums. (If you feel like it, try to also prove this without complex numbers.)

Problem 4.6 (Iberoamerican 2011)**.** Prove that, for any given positive integers $m \leq \ell$, there is a positive integer n and pairwise distinct positive integers $x_1, \cdots, x_n, y_1, \cdots, y_n$ such that the equality

$$\sum_{i=1}^{n} x_i^k = \sum_{i=1}^{n} y_i^k$$

holds for every $k = 1, 2, \ldots, m-1, m+1, \ldots, \ell$, but does not hold for $k = m$.

§4.2 Divided Differences

Problem 4.7. Check that the finite difference $\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} f(x+j)$ of f is $n!$ times the divided difference $f[x, x+1, x+2, \ldots, x+n]$.

Problem 4.8. Let f be a polynomial of degree d, and let $n > d$. Using the Lagrange Interpolation Formula

$$f(x) = \sum_{k=0}^{n} f(x_k) \frac{(x-x_0)\ldots(x-x_{k-1})(x-x_{k+1})\ldots(x-x_n)}{(x_k-x_0)(x_k-x_1)\ldots(x_k-x_{k-1})(x_k-x_{k+1})\ldots(x-x_n)},$$

give another proof that $f[x_0, x_1, \ldots, x_n]$ is always equal to zero[12].

Problem 4.9 (Based on Komal A.652.)**.** (a) Prove that if $f(x) = \frac{1}{x}$, then

$$f[x_0, x_1, \ldots, x_n] = \frac{(-1)^n}{x_0 x_1 \ldots x_n}.$$

(b) Prove that if positive integers $b_0 < b_1 < \cdots < b_n$ form an arithmetic progression, then

$$\operatorname{lcm}(b_0, b_1, \ldots, b_n) \geq \frac{b_0 b_1 \ldots b_n}{n!}.$$

(c) Compute the divided differences when $f(x) = \frac{1}{x^2}$.

Problem 4.10. Do there exist n periodic functions[13] $f_i : \mathbb{R} \to \mathbb{R}$ such that for all $x \in \mathbb{R}$,

$$x^n = f_1(x) + f_2(x) + \cdots + f_n(x) \quad ?$$

Problem 4.11. Let S be a set of odd integers. Prove that there exists a sequence of reals $(x_n)_{n=1}^{\infty}$ such that for every odd positive integer k, $\sum_{n=1}^{\infty} x_n^k$ converges if and only if $k \in S$.

[12] This is not necessarily the same thing as $f[x_0, x_1, \ldots, x_n]$ as an n-variate polynomial being identically zero, it only means that f always *evaluates* to $= 0$. But the Combinatorial Nullstellensatz proves that the two are in fact equivalent.

[13] By the way, each linear function is the sum of 2 periodic functions. I've heard that this generalizes; if you're interested, investigate how many periodic functions we need so that their sum could be x^n.

Problem 4.12 (Miklos Schweitzer 2014)**.** Let $n \geq 1$ be a fixed integer. Find the distance

$$\inf_{p,f} \max_{0 \leq x \leq 1} |f(x) - p(x)|,$$

where p runs over polynomials with real coefficients of degree less than n and f runs over functions $f(x) = \sum_{k=n}^{\infty} c_k x^k$ defined on the closed interval $[0, 1]$, where $c_k \geq 0$ and $f(1) = 1$.

If you'd like even more problems, take a look at `web.evanchen.cc/handouts/BMC_Combo_Null/BMC_Combo_Null.pdf`, or at the example problems in Problems From The Book by Andreescu and Dospinescu, Chapter 11 (Lagrange Interpolation Formula).

Thanks for reading!