Some Algebraic Combinatorics Arising in CR Geometry

John P. D'Angelo

University of Illinois at Urbana-Champaign

October 24, 2019

Plan of talk:

- Pascal's triangle revisited
- Roots of unity
- The invariant polynomial
- The other triangles
- Primality test
- Link to CR Geometry

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 **28** **56** 70 56 28 8 1

1 9 36 **84** 126 126 84 36 9 1

We all know the first order recurrence:

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

Combinatorial proof: How many ways can we choose $k+1$ people from a collection of $n+1$ people?
Either I am included: $\binom{n}{k}$ ways, or I am excluded: $\binom{n}{k+1}$ ways.

We all know the first order recurrence:

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

Combinatorial proof: How many ways can we choose $k+1$ people from a collection of $n+1$ people?
Either I am included: $\binom{n}{k}$ ways, or I am excluded: $\binom{n}{k+1}$ ways.

Algebraic proof:

$$\sum_{j=0}^{n+1} \binom{n+1}{j} x^j y^{n+1-j} = (x+y)^{n+1} =$$

$$(x+y)(x+y)^n = (x+y) \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}.$$

Now equate coefficients of $x^{k+1} y^{n-k}$.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 **6** 15 20 15 6 1

1 7 **21** 35 35 21 7 1

1 8 28 **56** 70 56 28 8 1

1 9 36 **84** 126 126 84 36 9 1

To verify this recurrence, iterate the usual one:

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = \binom{n}{k} + \binom{n-1}{k-1} + \binom{n-1}{k-2}$$

$$= \sum_{j=0}^{k} \binom{n-j}{k-j}.$$

We will describe infinitely many other triangles of integers that involve similar recurrences. These triangles will share other properties with Pascal's triangle. There will be only one other special triangle, where all the integers are positive.
We will put these things into a general accessible package.

A well-known fact about Pascal's triangle:
Except for the leading and final 1, all the entries in the row

$$1 \quad p \quad p(p-1)/2 \quad p(p-1)(p-2)/6 \quad \cdots$$

are divisible by p if and only if p is prime (or $p = 1$):
A freshman's dream:

$$(x+y)^p \cong x^p + y^p \mod (p)$$

if and only if p is prime (or $p = 1$).

A well-known fact about Pascal's triangle:
Except for the leading and final 1, all the entries in the row

$$1 \quad p \quad p(p-1)/2 \quad p(p-1)(p-2)/6 \quad \cdots$$

are divisible by p if and only if p is prime (or $p = 1$):
A freshman's dream:

$$(x+y)^p \cong x^p + y^p \mod (p)$$

if and only if p is prime (or $p = 1$).

Our infinitely many other triangles satisfy this property as well.

roots of unity

Consider a primitive m-th root of unity ω. We have

$$z^m - 1 = (z-1)(z-\omega)(z-\omega^2)...(z-\omega^{m-1}). \qquad (1)$$

Why? The roots of the equation are the powers of ω.

roots of unity

Consider a primitive m-th root of unity ω. We have

$$z^m - 1 = (z-1)(z-\omega)(z-\omega^2)...(z-\omega^{m-1}). \qquad (1)$$

Why? The roots of the equation are the powers of ω.
Replace z by $\frac{1}{z}$ in (1). Multiply on the left-hand side by z^m and each term on the right-hand side by z. We get

$$1 - z^m = (1-z)(1-\omega z)(1-\omega^2 z)...(1-\omega^{m-1} z). \qquad (1.1)$$

We will be generalizing (1.1).

roots of unity

Consider a primitive m-th root of unity ω. We have

$$z^m - 1 = (z-1)(z-\omega)(z-\omega^2)...(z-\omega^{m-1}). \qquad (1)$$

Why? The roots of the equation are the powers of ω.
Replace z by $\frac{1}{z}$ in (1). Multiply on the left-hand side by z^m and each term on the right-hand side by z. We get

$$1 - z^m = (1-z)(1-\omega z)(1-\omega^2 z)...(1-\omega^{m-1} z). \qquad (1.1)$$

We will be generalizing (1.1).
The set

$$\{1, \omega, \omega^2, ..., \omega^{m-1}\}$$

is a cyclic group of order m. Here $\omega^{-1} = \overline{\omega} = \omega^{m-1}$.

Rewrite (1.1):

$$\phi(z) = 1 - \prod_{j=0}^{m-1} (1 - \omega^j z) = 1 - (1 - z^m) = z^m. \qquad (2.1)$$

The main unifying theme of this talk is the generalization of (2.1) to other groups.

Rewrite (1.1):

$$\phi(z) = 1 - \prod_{j=0}^{m-1} (1 - \omega^j z) = 1 - (1 - z^m) = z^m. \qquad (2.1)$$

The main unifying theme of this talk is the generalization of (2.1) to other groups.

Second proof of (2.1):
ϕ is a polynomial of degree m in z.
It is invariant under the transformation $z \to \omega z$. Hence it can contain only the monomial z^m and constants. Thus

$$\phi(z) = a + bz^m.$$

Evaluating (2.1) at $z = 0$ gives 0. Thus $a = 0$.
Evaluating (2.1) at $z = 1$ gives 1. Thus $b = 1$ and $\phi(z) = z^m$.

Consider a simple generalization of (2.1):

$$(x+y)^m = 1 - \prod_{j=0}^{m-1} (1 - \omega^j x - \omega^j y). \tag{2.2}$$

Here we have the cyclic group of order m represented as 2-by-2 matrices:

$$\omega I = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}.$$

The group consists of

$$I, \omega I, \omega^2 I, ..., \omega^{m-1} I.$$

Consider a simple generalization of (2.1):

$$(x+y)^m = 1 - \prod_{j=0}^{m-1} (1 - \omega^j x - \omega^j y). \tag{2.2}$$

Here we have the cyclic group of order m represented as 2-by-2 matrices:

$$\omega I = \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}.$$

The group consists of

$$I, \omega I, \omega^2 I, ..., \omega^{m-1} I.$$

$$(x+y)^m = 1 - \prod_{j=0}^{m-1} (1 - \omega^j x - \omega^j y)$$

Thus Pascal's triangle is related to group invariance.

Invariant polynomials

The theme will be to generalize (2.2) to the abstract expression

$$1 - \prod_{\gamma \in \Gamma} (1 - \langle \gamma z, z \rangle) = \Phi_\Gamma(z, \overline{z}). \tag{3}$$

Here Γ will be a finite group of unitary matrices.

Invariant polynomials

The theme will be to generalize (2.2) to the abstract expression

$$1 - \prod_{\gamma \in \Gamma} (1 - \langle \gamma z, z \rangle) = \Phi_\Gamma(z, \overline{z}). \tag{3}$$

Here Γ will be a finite group of unitary matrices.

We cannot do much with the circle, because it is Abelian and the only finite subgroups are cyclic.
We will work with unitary matrices, usually 2-by-2.
The inner product:

$$\langle z, w \rangle = \sum_{j=1}^{n} z_j \overline{w}_j.$$

U is unitary if and only if $\langle Uz, Uw \rangle = \langle z, w \rangle$ for all z, w.

Assume that ω is a primitive p-th root of unity. For each q with $1 \leq q \leq p-1$ we consider a different representation of the cyclic group of order p:

$$\gamma = \begin{pmatrix} \omega & 0 \\ 0 & \omega^q \end{pmatrix}.$$

Mimicking (2.2) we obtain the following function:

$$f_{p,q}(x,y) = 1 - \prod_{j=0}^{p-1} (1 - \omega^j x - \omega^{qj} y).$$

These group-invariant maps have remarkable number-theoretic properties. When $q = 1$ we get Pascal's triangle. For $q = 2$, we get

1 1

1 3 1

1 5 5 1

1 7 14 7 1

1 **9** 27 30 9 1

1 11 **44** 77 55 11 1

1 13 **65** **156** 182 91 13 1

1 15 90 **275** 450 378 140 15 1

The previous triangle satisfies a third order recurrence (a second order recurrence if we ignore the final 1). Can you find a way to get the next row from the two rows above it?

The previous triangle satisfies a third order recurrence (a second order recurrence if we ignore the final 1). Can you find a way to get the next row from the two rows above it?

$$275 = 2(65) + 156 - 11.$$

$$450 = 2(156) + 182 - 44.$$

Hence the following polynomials equal one when we put $y = 1 - x$. Not obvious!

$$x^5 + 5x^3y + 5xy^2 + y^5$$

$$x^9 + 9x^7y + 27x^5y^2 + 30x^3y^3 + 9xy^4 + y^9$$

$$x^{15} + 15x^{13}y + 90x^{11}y^2 + 275x^9y^3 + 450x^7y^4 +$$
$$378x^5y^5 + 140x^3y^6 + 15xy^7 + y^{15}$$

The polynomial $f_{p,2}$ satisfies

$$f_{p,2}(x, y) \cong x^p + y^p \mod (p)$$

if and only if p is prime.

The polynomial $f_{p,2}$ satisfies

$$f_{p,2}(x, y) \cong x^p + y^p \mod (p)$$

if and only if p is prime.

Theorem

For each q,

$$f_{p,q}(x, y) \cong x^p + y^p \mod (p)$$

if and only if $p = 1$ or p is prime.

What happens for $q = 3$?

$$1\ 1$$

$$1\ 2\ 1$$

$$1\ 3\ -3\ 1$$

$$1\ 4\ -2\ 1$$

$$1\ 5\ 5\ 1$$

$$1\ 6\ 3\ 2\ -3\ 1$$

$$1\ 7\ 7\ -7\ 1$$

$$1\ 8\ 12\ -2\ 8\ 1$$

$$1\ 9\ 18\ 3\ 9\ -3\ 1$$

$$1\ 10\ 25\ 10\ 2\ -15\ 1$$

$$1\ 11\ 33\ 22\ -11\ 11\ 1$$

What happens for $q = 3$?

$$1\ 1$$
$$1\ 2\ 1$$
$$1\ 3\ -3\ 1$$
$$1\ 4\ -2\ 1$$
$$1\ 5\ 5\ 1$$
$$1\ 6\ 3\ 2\ -3\ 1$$
$$1\ 7\ 7\ -7\ 1$$
$$1\ 8\ 12\ -2\ 8\ 1$$
$$1\ 9\ 18\ 3\ 9\ -3\ 1$$
$$1\ 10\ 25\ 10\ 2\ -15\ 1$$
$$1\ 11\ 33\ 22\ -11\ 11\ 1$$

We get some negative coefficients. Grundmeier proved: For $q \geq 3$, asympotically $\frac{1}{4}$ of the coefficients are negative.

What happens for $q = 3$?

$$1\ 1$$
$$1\ 2\ 1$$
$$1\ 3\ -3\ 1$$
$$1\ 4\ -2\ 1$$
$$1\ 5\ 5\ 1$$
$$1\ 6\ 3\ 2\ -3\ 1$$
$$1\ 7\ 7\ -7\ 1$$
$$1\ 8\ 12\ -2\ 8\ 1$$
$$1\ 9\ 18\ 3\ 9\ -3\ 1$$
$$1\ 10\ 25\ 10\ 2\ -15\ 1$$
$$1\ 11\ 33\ 22\ -11\ 11\ 1$$

We get some negative coefficients. Grundmeier proved: For $q \geq 3$, asympotically $\frac{1}{4}$ of the coefficients are negative.

The primality property holds and there is a 7-th order recurrence.

Proof of the primality test

The key idea is orthogonal homogenization. For these polynomials, this idea is easy. By invariance we have

$$f_{p,q}(x,y) = x^p + y^p + \sum_k c_k x^{p-qk} y^k.$$

Since $f_{p,q}(x,y) = 1$ when $x + y = 1$ we get

$$x^p + y^p + \sum_k c_k x^{p-qk} y^k (x+y)^{k(q-1)} = (x+y)^p. \qquad (*)$$

Proof of the primality test

The key idea is orthogonal homogenization. For these polynomials, this idea is easy. By invariance we have

$$f_{p,q}(x,y) = x^p + y^p + \sum_k c_k x^{p-qk} y^k.$$

Since $f_{p,q}(x,y) = 1$ when $x + y = 1$ we get

$$x^p + y^p + \sum_k c_k x^{p-qk} y^k (x+y)^{k(q-1)} = (x+y)^p. \qquad (*)$$

Thus, if the coefficients are 0 mod (p), they remain so upon homogenization. We get that $p = 1$ or p is prime.

Proof of the primality test

The key idea is orthogonal homogenization. For these polynomials, this idea is easy. By invariance we have

$$f_{p,q}(x,y) = x^p + y^p + \sum_k c_k x^{p-qk} y^k.$$

Since $f_{p,q}(x,y) = 1$ when $x + y = 1$ we get

$$x^p + y^p + \sum_k c_k x^{p-qk} y^k (x+y)^{k(q-1)} = (x+y)^p. \qquad (*)$$

Thus, if the coefficients are 0 mod (p), they remain so upon homogenization. We get that $p = 1$ or p is prime.
Converse is slightly harder. When p is prime $\mathbb{Z}/p\mathbb{Z}$ is a field. The polynomials arising in (*) have different degrees in x and hence are linearly independent. Hence a linear combination of them being 0 means that each is 0 and the result follows.

Why do the polynomials for different groups have anything to do with each other?

Why do the polynomials for different groups have anything to do with each other?

Think of $f(w^j) = (1 - xw^j - yw^{qj})$ as a polynomial in w, evaluated at w^j. We have

$$1 - \prod_0^{p-1} f(w^j) = 1 - \prod_0^{p-1} \prod_{k=1}^{q} (1 - c_k(x,y)w^j).$$

Interchange order of product.

$$= 1 - \prod_1^{q} \prod_0^{p-1} (1 - c_k(x,y)w^j).$$

Why do the polynomials for different groups have anything to do with each other?

Think of $f(w^j) = (1 - xw^j - yw^{qj})$ as a polynomial in w, evaluated at w^j. We have

$$1 - \prod_0^{p-1} f(w^j) = 1 - \prod_0^{p-1} \prod_{k=1}^{q} (1 - c_k(x,y)w^j).$$

Interchange order of product.

$$= 1 - \prod_1^{q} \prod_0^{p-1} (1 - c_k(x,y)w^j).$$

But we know how to find the inner (no pun intended) product.

$$\prod_{j=0}^{p-1} (1 - zw^j) = 1 - z^p \tag{1.1}$$

Putting it all together we get

$$f_{p,q}(x,y) = 1 - \prod_{1}^{q}(1 - c_k(x,y)^p)$$

$$= \sum c_k^p - \sum (c_k c_l)^p + \sum (c_k c_l c_m)^p - \cdots$$

Everything comes down to finding the (reciprocals of the) roots of

$$(1 - xw - yw^q).$$

No closed formula in general, of course.

Conclusion: Everything works for any polynomial whose coefficients are regarded as variables. We can express everything in terms of the roots, but there is no closed formula for the roots as functions of the coefficients.

Conclusion: Everything works for any polynomial whose coefficients are regarded as variables. We can express everything in terms of the roots, but there is no closed formula for the roots as functions of the coefficients.

Pascal's triangle used $(1 - xw - yw)$.
The next triangle used $(1 - xw - yw^2)$.
The third triangle used $(1 - xw - yw^3)$.

Conclusion: Everything works for any polynomial whose coefficients are regarded as variables. We can express everything in terms of the roots, but there is no closed formula for the roots as functions of the coefficients.

Pascal's triangle used $(1 - xw - yw)$.
The next triangle used $(1 - xw - yw^2)$.
The third triangle used $(1 - xw - yw^3)$.
In principle one can do something similar for any finite subgroup of unitary matrices.

How do these ideas lead to several complex variables and CR Geometry?
Unitary maps preserve the unit sphere. Let $\Gamma \subseteq U(n)$ be a finite subgroup. It makes sense to consider invariant maps on the unit sphere.
For what finite subgroups Γ of $U(n)$ is there a non-constant invariant rational map taking the unit sphere to some unit sphere?

Theorem (Lichtblau)

(1992) Assume $\Gamma \subset U(n)$ is a finite subgroup. If there is a non-constant Γ-invariant rational holomorphic map from S^{2n-1} to some S^{2N-1}, then Γ is cyclic.

Theorem

If there is a non-constant complex analytic Γ*-invariant map from* S^{2n-1} *to a sphere, then* Γ *must be represented in a special way.*

Let η be a primitive p-th root of unity. The only possibilities are the groups generated by:

$$\eta I \tag{9.1}$$

$$\begin{pmatrix} \eta & 0 \\ 0 & \eta^2 \end{pmatrix} \quad p \text{ odd} \tag{9.2}$$

$$\begin{pmatrix} \eta & 0 & 0 \\ 0 & \eta^2 & 0 \\ 0 & 0 & \eta^4 \end{pmatrix} \quad p = 7 \tag{9.3}$$

When $n = 2$, (9.1) leads to
$f_{p,1}(x, y) = (x + y)^p = (|z|^2 + |w|^2)^p = 1.$
(9.2) leads to

$$f_{p,2}(x, y) = (\frac{x + \sqrt{x^2 + 4y}}{2})^p + (\frac{x - \sqrt{x^2 + 4y}}{2})^p + y^p.$$

These are the polynomials we saw before such as

$$x^5 + 5x^3y + 5xy^2 + y^5.$$

(9.3) is a kind of conglomeration of (9.2). Works only if $\eta^7 = 1$.

CR Geometry

CR Geometry studies real objects in complex spaces.
Basic example: odd dimensional unit sphere S^{2n-1}.
A CR mapping is an analogue of a complex analytic mapping. It depends on z but not on $\overline{z}$.
In a good complex variables course, one can cop z's but not z-bars....

The interaction between the degrees of rational maps from S^{2n-1} to S^{2N-1} in terms of n, N leads to a new field of mathematics, CR complexity theory. Furthermore, the group invariant maps $f_{p,2}$ are extremal. Proof uses directed graphs, sources, and sinks.
They are of degree $p = 2r + 1$ and have $r + 2$ terms.

To obtain group-invariant maps, one must replace the target sphere with a hyperquadric.

$$Q(A,B) = \{z : \sum_{j=1}^{A} |z_j|^2 - \sum_{j=A+1}^{A+B} |z_j|^2 = 1\}.$$

Theorem

Given any finite subgroup Γ of $U(n)$ there is a Γ-invariant polynomial (complex analytic) map from S^{2n-1} to some hyperquadric.

It comes from the invariant polynomial Φ_Γ.

We need enough eigenvalues of both signs. My former student Grundmeier has done lots of work on this problem.
For example: the target hyperquadric for the binary icosahedral group has 40 positive, 22 negative eigenvalues.
These invariant polynomials have taken us from Pascal's triangle to CR Geometry!

Return to our first triangle

Putting $x = |z_1|^2$ and $y = |z_2|^2$ yields a polynomial $f(x, y) = f_{p,2}(x, y)$ in two real variables x, y with these properties:

- $f(x, y) = 1$ on $x + y = 1$. (sphere)
- $f(\omega x, \omega^2 y) = f(x, y)$. (invariance)
- f has degree p.
- f has $r + 2$ positive terms and no negative terms if $p = 2r + 1$ is odd.
- f has $r + 1$ positive and 1 negative term (namely $-y^p$) if $p = 2r$ is even.
- $f(x, y)$ has integer coefficients.
- $f(x, y)$ is congruent to $x^p + y^p$ modulo p if and only if p is prime (or $p = 1$).

In fact, f has the explicit formula

$$(\frac{x+\sqrt{x^2+4y}}{2})^p + (\frac{x-\sqrt{x^2+4y}}{2})^p + (-1)^{p+1}y^p.$$

Same ideas works for all representations of cyclic subgroups of $U(2)$, but the formulas are not explicit.

For the polynomials $1 - \prod_{j=0}^{p-1}(1 - \eta^j x - \eta^{qj} y)$,
Loehr, Warrington, Wilf gave a combinatorial interpretation of the coefficients.

Theorem

The coefficient $c_{p,q}(r,s)$ is equal, aside from its sign, to the number of permutations σ of p letters such that for $j = 1, \ldots, p$ the differences $\sigma(j) - j$ mod (p) take the values $0, 1, q$ with respective multiplicities $p - r - s, r, s$. Furthermore, these permutations all have the same sign and the same cycle type.

For the polynomials $1 - \prod_{j=0}^{p-1}(1 - \eta^{q_1 j}x - \eta^{q_2 j}y)$,
Grundmeier, Linsuain, Whitaker proved:

Theorem

Suppose $gcd(p, q1, q2) = 1$. *The monomials* $x^r y^s$ *which appear are exactly those for which* $p|(rq_1 + sq_2)$, *and the coefficients are positive if and only if* $gcd(q_1, q_2, rq_1 + sq_2)$ *is odd.*

They also generalized LWW to this situation.