Polynomials in Combinatorics: Four Examples

Yaokun Wu (吴耀琨)

Department of Mathematics, Shanghai Jiao Tong University
ykwu@sjtu.edu.cn

April 3, 2008

Combinatorial Structures

Many facts and problems in mathematics, computer science, and engineering are most easily stated in terms of five combinatorial structures: 1. graphs, 2. directed graphs, 3. partially ordered sets, 4. simplicial complexes, 5. matroids. We will devote one chapter to each of these structures and a sixth chapter to computational complexity, in order to illuminate the relative difficulty of well-known problems. Since the definition of our five structures are simple and very closely related, it is somewhat surprising that they rarely appear together in an introductory combinatorics text. – Mark Skandera, Introduction to Combinatorics and Graph Theory, Lecture Notes, 2003.

Polynomials

Linear Algebra is concerned with polynomials of degree one.

Algebraic Geometry is the study of systems of polynomial equations in one or more variables, combining the algebraic with the geometric for the benefit of both.

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B;

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B; To show $|A| \leq |B|$ is just to show the existence of an injective map from A to B.

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B; To show $|A| \leq |B|$ is just to show the existence of an injective map from A to B.

Consider an $\mathcal{F}$-vectorspace V of dimension m.
To show $|A| \geq m$ is just to show the existence of an injective linear map from V to $\mathcal{F}^A$;

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B; To show $|A| \leq |B|$ is just to show the existence of an injective map from A to B.

Consider an $\mathcal{F}$-vectorspace V of dimension m.
To show $|A| \geq m$ is just to show the existence of an injective linear map from V to $\mathcal{F}^A$; To show $|A| \leq m$ is just to show the existence of an injective linear map from $\mathcal{F}^A$ to V.

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B; To show $|A| \leq |B|$ is just to show the existence of an injective map from A to B.

Consider an $\mathcal{F}$-vectorspace V of dimension m.
To show $|A| \geq m$ is just to show the existence of an injective linear map from V to $\mathcal{F}^A$; To show $|A| \leq m$ is just to show the existence of an injective linear map from $\mathcal{F}^A$ to V.

We could turn to surjective linear maps instead. But many nice examples are really involved with injective ones.

Dimension Argument

To show $|A| \geq |B|$ is just to show the existence of a surjective map from A to B; To show $|A| \leq |B|$ is just to show the existence of an injective map from A to B.

Consider an $\mathcal{F}$-vectorspace V of dimension m.
To show $|A| \geq m$ is just to show the existence of an injective linear map from V to $\mathcal{F}^A$; To show $|A| \leq m$ is just to show the existence of an injective linear map from $\mathcal{F}^A$ to V.

We could turn to surjective linear maps instead. But many nice examples are really involved with injective ones.

When V is some linear space consisting of polynomials, the above idea falls inside the scope of polynomial method.

Outline

Let $\mathcal{F}$ be a finite field. A Kakeya set in $\mathcal{F}^n$ is a set $E \subseteq \mathcal{F}^n$ which contains a line in each direction, namely for any $v \in \mathcal{F}^n$ there exists $x_v \in E$ such that

$$\{x_v + tv : \ t \in \mathcal{F}\} \subseteq E. \tag{1}$$

Let $\mathcal{F}$ be a finite field. A Kakeya set in $\mathcal{F}^n$ is a set $E \subseteq \mathcal{F}^n$ which contains a line in each direction, namely for any $v \in \mathcal{F}^n$ there exists $x_v \in E$ such that

$$\{x_v + tv : \ t \in \mathcal{F}\} \subseteq E. \tag{1}$$

Theorem 1 (Zeev Dvir, Mar. 20, 2008)

Every Kakeya set in $\mathcal{F}^n$ has at least $\binom{|\mathcal{F}|+n-1}{n}$ elements.

Let $\mathcal{F}$ be a finite field. A Kakeya set in $\mathcal{F}^n$ is a set $E \subseteq \mathcal{F}^n$ which contains a line in each direction, namely for any $v \in \mathcal{F}^n$ there exists $x_v \in E$ such that

$$\{x_v + tv : \ t \in \mathcal{F}\} \subseteq E. \tag{1}$$

Theorem 1 (Zeev Dvir, Mar. 20, 2008)

Every Kakeya set in $\mathcal{F}^n$ has at least $\binom{|\mathcal{F}|+n-1}{n}$ elements.

Note that $\binom{|\mathcal{F}|+n-1}{n} \geq \frac{|\mathcal{F}|^n}{n!}$. Thus a Kakeya set over any finite field must be 'full dimensional'.

Zeev Dvir, A Ph.D. Student at the department of Computer Science at the Weizmann Institute of Science.
http://www.wisdom.weizmann.ac.il/~zdvir/

Let $V_d \leq \mathcal{F}[v_1, \ldots, v_n]$ be the $\mathcal{F}$-vectorspace of all polynomials in n variables $v_1, \ldots, v_n$ whose degrees are no greater than d. We regard $V_d = \{0\}$ for any $d < 0$.

Lemma 2

$\dim V_d = \binom{n+d}{n}$.

Proof.

When $n = 4, d = 7$, we construct a map which sends $v_1^2 v_2^0 v_3^1 v_4^2$ to $bbrrbrbbrbb$. □

Let $V_d \leq \mathcal{F}[v_1, \ldots, v_n]$ be the $\mathcal{F}$-vectorspace of all polynomials in n variables $v_1, \ldots, v_n$ whose degrees are no greater than d. We regard $V_d = \{0\}$ for any $d < 0$.

Lemma 2

$\dim V_d = \binom{n+d}{n}$.

Proof.

When $n = 4, d = 7$, we construct a map which sends $v_1^2 v_2^0 v_3^1 v_4^2$ to $bbrrbrbbrbb$. □

Exercise 3

The number of monomials in $\mathcal{F}[v_1, \ldots, v_n]$ of degree exactly d follows readily from Lemma 2. Please try to provide a bijective proof.

Lemma 4

Let E be a Kakeya set in $\mathcal{F}^n$. Then the natural map f from $V_{|\mathcal{F}|-1}$ to $\mathcal{F}^E$ which sends P to $P|_E$ is an injective linear map.

Proof.

Take $P \in V_{|\mathcal{F}|-1}$ which vanishes on E.

Lemma 4

Let E be a Kakeya set in $\mathcal{F}^n$. Then the natural map f from $V_{|\mathcal{F}|-1}$ to $\mathcal{F}^E$ which sends P to $P|_E$ is an injective linear map.

Proof.

Take $P \in V_{|\mathcal{F}|-1}$ which vanishes on E. Let $P = P_d + P' \in V_d$, where $d \leq |\mathcal{F}| - 1$, $P' \in V_{d-1}$. To prove $P = 0$, we need only demonstrate that $P_d = 0$,

Lemma 4

Let E be a Kakeya set in $\mathcal{F}^n$. Then the natural map f from $V_{|\mathcal{F}|-1}$ to $\mathcal{F}^E$ which sends P to $P|_E$ is an injective linear map.

Proof.

Take $P \in V_{|\mathcal{F}|-1}$ which vanishes on E. Let $P = P_d + P' \in V_d$, where $d \leq |\mathcal{F}| - 1$, $P' \in V_{d-1}$. To prove $P = 0$, we need only demonstrate that $P_d = 0$, or equivalently P_d vanishes on $\mathcal{F}^n$, due to $d < |\mathcal{F}|$.

Lemma 4

Let E be a Kakeya set in $\mathcal{F}^n$. Then the natural map f from $V_{|\mathcal{F}|-1}$ to $\mathcal{F}^E$ which sends P to $P|_E$ is an injective linear map.

Proof.

Take $P \in V_{|\mathcal{F}|-1}$ which vanishes on E. Let $P = P_d + P' \in V_d$, where $d \leq |\mathcal{F}| - 1$, $P' \in V_{d-1}$. To prove $P = 0$, we need only demonstrate that $P_d = 0$, or equivalently P_d vanishes on $\mathcal{F}^n$, due to $d < |\mathcal{F}|$. For any $v \in \mathcal{F}^n$, we deduce from Eq. (1) that for any $t \in \mathcal{F}$, $0 = P(x_v + tv) = P_d(v)t^d + Q$, where Q is a polynomial in t of degree at most $d - 1$ and with coefficients in $\mathcal{F}[v_1, \ldots, v_n]$.

Lemma 4

Let E be a Kakeya set in $\mathcal{F}^n$. Then the natural map f from $V_{|\mathcal{F}|-1}$ to $\mathcal{F}^E$ which sends P to $P|_E$ is an injective linear map.

Proof.

Take $P \in V_{|\mathcal{F}|-1}$ which vanishes on E. Let $P = P_d + P' \in V_d$, where $d \leq |\mathcal{F}| - 1$, $P' \in V_{d-1}$. To prove $P = 0$, we need only demonstrate that $P_d = 0$, or equivalently P_d vanishes on $\mathcal{F}^n$, due to $d < |\mathcal{F}|$. For any $v \in \mathcal{F}^n$, we deduce from Eq. (1) that for any $t \in \mathcal{F}$, $0 = P(x_v + tv) = P_d(v)t^d + Q$, where Q is a polynomial in t of degree at most $d - 1$ and with coefficients in $\mathcal{F}[v_1, \ldots, v_n]$. This gives $P_d(v) = 0$, finishing the proof. □

The key to the proof of Lemma 4 and many other similar work is the fact that nonzero polynomials do not have many distinct roots.

The key to the proof of Lemma 4 and many other similar work is the fact that nonzero polynomials do not have many distinct roots.Both ‘nonzero’ and ‘many’ can be understood in many senses.

The key to the proof of Lemma 4 and many other similar work is the fact that nonzero polynomials do not have many distinct roots.Both 'nonzero' and 'many' can be understood in many senses.

Do you get a proof of Theorem 1 now?

A set $B \subseteq \mathcal{F}^n$ is a Nikodym set provided for each $v \notin B$ there is a line L such that $L \setminus B = \{v\}$.

Theorem 5 (李良攀, Mar. 25, 2008)

Any Nikodym set B in $\mathcal{F}^n$ must have a size at least $\binom{n+|\mathcal{F}|-2}{n}$.

A set $B \subseteq \mathcal{F}^n$ is a Nikodym set provided for each $v \notin B$ there is a line L such that $L \setminus B = \{v\}$.

Theorem 5 (李良攀, Mar. 25, 2008)

Any Nikodym set B in $\mathcal{F}^n$ must have a size at least $\binom{n+|\mathcal{F}|-2}{n}$.

Proof.

By Lemma 2, it suffices to show that if $P \in V_{|\mathcal{F}|-2}$ vanishes on B, it must vanish everywhere.

A set $B \subseteq \mathcal{F}^n$ is a Nikodym set provided for each $v \notin B$ there is a line L such that $L \setminus B = \{v\}$.

Theorem 5 (李良攀, Mar. 25, 2008)

Any Nikodym set B in $\mathcal{F}^n$ must have a size at least $\binom{n+|\mathcal{F}|-2}{n}$.

Proof.

By Lemma 2, it suffices to show that if $P \in V_{|\mathcal{F}|-2}$ vanishes on B, it must vanish everywhere. Take $v \notin B$ and let us see how can we get $P(v) = 0$.

A set $B \subseteq \mathcal{F}^n$ is a Nikodym set provided for each $v \notin B$ there is a line L such that $L \setminus B = \{v\}$.

Theorem 5 (李良攀, Mar. 25, 2008)

Any Nikodym set B in $\mathcal{F}^n$ must have a size at least $\binom{n+|\mathcal{F}|-2}{n}$.

Proof.

By Lemma 2, it suffices to show that if $P \in V_{|\mathcal{F}|-2}$ vanishes on B, it must vanish everywhere. Take $v \notin B$ and let us see how can we get $P(v) = 0$. Choose $x \in \mathcal{F}^n \setminus \{0\}$ such that $v + tx \in B$ for all $t \in \mathcal{F} \setminus \{0\}$. $P(v + tx)$, as a polynomial in t of degree at most $|\mathcal{F}| - 2$ which has at least $|\mathcal{F}| - 1$ different roots, must vanish indeed for all $t \in \mathcal{F}$ and so $P(v) = 0$ is obtained. □

Theorem 6

If R^n is covered by m sets with $m < (1 + o(1))(1.2)^n$ then there is one set within which all the distances are realised.

Theorem 6

If R^n is covered by m sets with $m < (1 + o(1))(1.2)^n$ then there is one set within which all the distances are realised.

The above nice result was proved in:

P. Frankl, R. Wilson, Intersection theorems with geometric consequences, Combinatorica 1 (1981), 357–368.

Theorem 6

If R^n is covered by m sets with $m < (1 + o(1))(1.2)^n$ then there is one set within which all the distances are realised.

The above nice result was proved in:

P. Frankl, R. Wilson, Intersection theorems with geometric consequences, Combinatorica 1 (1981), 357–368.

To prove Theorem 6, Frankl and Wilson established an upper bound for the size of a set system with restricted pairwise intersection sizes. We state here a generalization of this result. Note that we always use $[n]$ for $\{1, \ldots, n\}$.

To prove Theorem 6, Frankl and Wilson established an upper bound for the size of a set system with restricted pairwise intersection sizes. We state here a generalization of this result. Note that we always use $[n]$ for $\{1, \ldots, n\}$.

Theorem 7 (Deza-Frankl-Singhi, 1983)

Let p be a prime, n a positive integer, and L a set of s integers. Let $\mathcal{H} \subseteq 2^{[n]}$ such that for any $A \neq B \in \mathcal{H}$, we have $|A \cap B| \in L \pmod p$ and $|A| \notin L \pmod p$. Then $|\mathcal{H}| \leq \sum_{k=0}^{s} \binom{n}{k}$.

Theorem 8 (Alon-Babai-Suzuki, 1991)

Let $\mathcal{H} \subseteq 2^{[n]}$ *such that for any* $A \neq B \in \mathcal{H}$, *we have* $|A \cap B| \in \{\lambda_1, \ldots, \lambda_s\}$. *Then* $|\mathcal{H}| \leq \sum_{k=0}^{s} \binom{n}{k}$.

Theorem 8 (Alon-Babai-Suzuki, 1991)

Let $\mathcal{H} \subseteq 2^{[n]}$ such that for any $A \neq B \in \mathcal{H}$, we have $|A \cap B| \in \{\lambda_1, \ldots, \lambda_s\}$. Then $|\mathcal{H}| \leq \sum_{k=0}^{s} \binom{n}{k}$.

Next: how shall we define the whale, by his obvious externals, so as conspicuously to label him for all time to come. To be short, then, a whale is a spouting fish with a horizontal tail. There you have him. However contracted, that definition is the result of expanded meditation. – Moby Dick; or The Whale 白鲸记, Herman Melville 赫尔曼.梅尔维尔(1819-1891)

Proof of Theorem 8

Suppose $\mathcal{H} = \{A_1, \ldots, A_m\}$ with $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$.
Put X_i to be the characteristic vector of A_i, $i \in [m]$.

Proof of Theorem 8

Suppose $\mathcal{H} = \{A_1, \ldots, A_m\}$ with $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. Put X_i to be the characteristic vector of A_i, $i \in [m]$. Define the polynomial $f_i \in R[v_1, \ldots, v_m]$, $i \in [m]$, by setting

$$f_i(v) = \prod_{j:\lambda_j < |A_i|} (v \cdot X_i - \lambda_j).$$

We adopt the convention that $\prod_{j \in \emptyset}(v \cdot X_i - \lambda_j) = 1$.

Proof of Theorem 8

Suppose $\mathcal{H} = \{A_1, \ldots, A_m\}$ with $|A_1| \leq |A_2| \leq \cdots \leq |A_m|$. Put X_i to be the characteristic vector of A_i, $i \in [m]$. Define the polynomial $f_i \in R[v_1, \ldots, v_m]$, $i \in [m]$, by setting

$$f_i(v) = \prod_{j:\lambda_j < |A_i|} (v \cdot X_i - \lambda_j).$$

We adopt the convention that $\prod_{j \in \emptyset}(v \cdot X_i - \lambda_j) = 1$. Define g_i to be the multilinear polynomial which takes the same value with f_i on $\{0,1\}^n$, $i \in [m]$. (Note that $v_1^6 v_2 v_4^2|_{\{0,1\}^4} = v_1 v_2 v_4|_{\{0,1\}^4}$.)

Proof of Theorem 8, Contd.

Observe that

$$M = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} \begin{pmatrix} X_1 & \cdots & X_m \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \begin{pmatrix} X_1 & \cdots & X_m \end{pmatrix}.$$

is an upper triangular matrix whose diagonal is occupied by positive numbers.

To see this, just check that

$$f_i(X_i) = \prod_{j:\lambda_j<|A_i|} (|A_i| - \lambda_j) > 0$$

Proof of Theorem 8, Contd.

Observe that

$$M = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} \begin{pmatrix} X_1 & \cdots & X_m \end{pmatrix} = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix} \begin{pmatrix} X_1 & \cdots & X_m \end{pmatrix}.$$

is an upper triangular matrix whose diagonal is occupied by positive numbers.

To see this, just check that

$$f_i(X_i) = \prod_{j:\lambda_j<|A_i|} (|A_i| - \lambda_j) > 0$$

and that

$$f_{i+t}(X_i) = \prod_{j:\lambda_j<|A_{i+t}|} (X_i \cdot X_{i+t} - \lambda_j) = 0.$$

Proof of Theorem 8, Fin.

If $\sum_{i=1}^{m} c_i g_i = 0$, then $\sum_{i=1}^{m} c_i g_i(X_j) = 0$ for all j and hence $(c_1 \ \ldots \ c_m)M = 0$ follows. Since M is nonsingular, we know that $c_1 = \cdots = c_m = 0$.

Proof of Theorem 8, Fin.

If $\sum_{i=1}^{m} c_i g_i = 0$, then $\sum_{i=1}^{m} c_i g_i(X_j) = 0$ for all j and hence $(c_1 \ \ldots \ c_m)M = 0$ follows. Since M is nonsingular, we know that $c_1 = \cdots = c_m = 0$.

We thus find that $A_i \longrightarrow g_i$ gives rise to an injective linear map from $R^{\mathcal{H}}$ to the linear space $\mathscr{L}$ of multilinear polynomials in $v_1, \ldots, v_n$ with degrees at most s. It is easy to see that $\dim \mathscr{L} = \sum_{k=0}^{s} \binom{n}{k}$ and so we are done.

Exercise 9

Work out a proof of Theorem 7. Does it hold when p is not necessarily a prime?

Exercise 9

Work out a proof of Theorem 7. Does it hold when p is not necessarily a prime?

> *The pleasure we obtain from music comes from counting, but counting unconsciously. Music is nothing but unconscious arithmetic. —G.W. Leibniz*

A set $A \subseteq R^n$ is a two distance set if at most two positive distances are determined by different points of A. Denote by $f(n, 2)$ the maximum size of a two distance set in R^n.

Theorem 10

$f(n, 2) \leq \frac{(n+1)(n+4)}{2}$.

Exercise 11

Can you improve the bound given in Theorem 10?

Proof of Theorem 10

Let $A \subseteq R^n$ be a two-distance set with $|A| = f(n, 2)$ and let d_1, d_2 be the distinct distances determined by A. For every $a = (a_1 \ \ldots \ a_n) \in A$, we define $f_a \in R[v_1, \ldots, v_n]$ by putting

$$f_a(v_1, \ldots, v_n) = (\sum_{i=1}^{n}(v_i - a_i)^2 - d_1^2)(\sum_{i=1}^{n}(v_i - a_i)^2 - d_2^2).$$

We claim that $\{f_a : \ a \in A\}$ is linearly independent. (Did we just learn any method to accomplish this?

Proof of Theorem 10

Let $A \subseteq R^n$ be a two-distance set with $|A| = f(n, 2)$ and let d_1, d_2 be the distinct distances determined by A. For every $a = (a_1 \ \ldots \ a_n) \in A$, we define $f_a \in R[v_1, \ldots, v_n]$ by putting

$$f_a(v_1, \ldots, v_n) = (\sum_{i=1}^{n}(v_i - a_i)^2 - d_1^2)(\sum_{i=1}^{n}(v_i - a_i)^2 - d_2^2).$$

We claim that $\{f_a : \ a \in A\}$ is linearly independent. (Did we just learn any method to accomplish this? Yes, we did this kind of matter in the proof of Theorem 8!)

Proof of Theorem 10

Let $A \subseteq R^n$ be a two-distance set with $|A| = f(n, 2)$ and let d_1, d_2 be the distinct distances determined by A. For every $a = (a_1 \ \ldots \ a_n) \in A$, we define $f_a \in R[v_1, \ldots, v_n]$ by putting

$$f_a(v_1, \ldots, v_n) = (\sum_{i=1}^{n}(v_i - a_i)^2 - d_1^2)(\sum_{i=1}^{n}(v_i - a_i)^2 - d_2^2).$$

We claim that $\{f_a : \ a \in A\}$ is linearly independent. (Did we just learn any method to accomplish this? Yes, we did this kind of matter in the proof of Theorem 8!) We know that all f_a' lie in a linear space of dimension $1 + n + \binom{n+1}{2} + n + 1 = \frac{(n+1)(n+4)}{2}$. Why?

Proof of Theorem 10

Let $A \subseteq R^n$ be a two-distance set with $|A| = f(n, 2)$ and let d_1, d_2 be the distinct distances determined by A. For every $a = (a_1 \ \ldots \ a_n) \in A$, we define $f_a \in R[v_1, \ldots, v_n]$ by putting

$$f_a(v_1, \ldots, v_n) = (\sum_{i=1}^{n}(v_i - a_i)^2 - d_1^2)(\sum_{i=1}^{n}(v_i - a_i)^2 - d_2^2).$$

We claim that $\{f_a : \ a \in A\}$ is linearly independent. (Did we just learn any method to accomplish this? Yes, we did this kind of matter in the proof of Theorem 8!) We know that all f_a' lie in a linear space of dimension $1 + n + \binom{n+1}{2} + n + 1 = \frac{(n+1)(n+4)}{2}$. Why? Indeed, they lie in the linear space spanned by $\{(\sum_i v_i^2)^2, v_j(\sum_i v_i^2), v_i v_j, v_i, 1\}$.

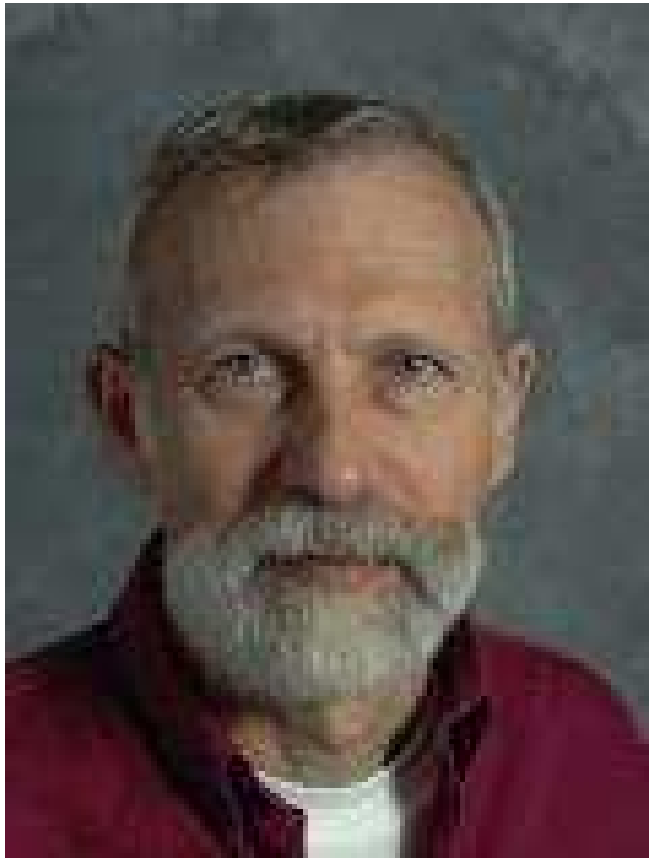
Teacher versus Researcher

http://www.math.rutgers.edu/people/Gelfand.html
Israil Gelfand (1978 Wolf Prize in Mathematics Laureate):

Teacher versus Researcher

`http://www.math.rutgers.edu/people/Gelfand.html`
Israil Gelfand (1978 Wolf Prize in Mathematics Laureate):

> *One of the characteristic features of Israil Moiseevic's activities has been the extremely close bond between his research work and his teaching. The formulation of new problems and unexpected questions, a tendency to look at even well known things from a new point of view characterises Gelfand as a teacher, regardless of whether at a given moment he is holding a conversation with schoolchildren or with his own colleagues.*



Hell is a boring incomprehensible math talk that goes overtime. – Harry Dym

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!

Thank You!!! 谢谢!!!