The $fg + 1$ problem for Newton polygons

Pascal Koiran

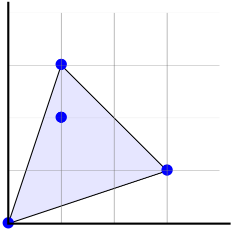
Lyon, April 2025

Based on joint work with:
Natacha Portier, Sébastien Tavenas and Stéphan Thomassé

(and also: William Aufort, Karthik C.S.)

The Newton polygon

- Let $f(X, Y) = \sum_i \alpha_i X^{a_i} Y^{b_i}$
- Monomials of f : $\mathrm{Mon}(f) = \{(a_i, b_i), \alpha_i \neq 0\}$
- The Newton polygon: $\mathrm{Newt}(f) = \mathrm{Conv}(\mathrm{Mon}(f))$
- An example: $f(X, Y) = 1 + 2X^3Y + XY^2 + XY^3$



The Newton polygon of $fg + 1$: a little puzzle

Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg + 1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$:

The Newton polygon of $fg + 1$: a little puzzle

Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg + 1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$:

The Newton polygon of $fg + 1$: a little puzzle

Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg + 1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$:

The Newton polygon of $fg + 1$: a little puzzle

Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg + 1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$: $2t$ is a tight upper bound.

The Newton polygon of $fg + 1$: a little puzzle

Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg + 1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$: $2t$ is a tight upper bound.

- **Lemma** [Ostrowski] : $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$.
  Minkowski sum: $P + Q = \{p + q, p \in P, q \in Q\}$.

The Newton polygon of $fg + 1$: a little puzzle

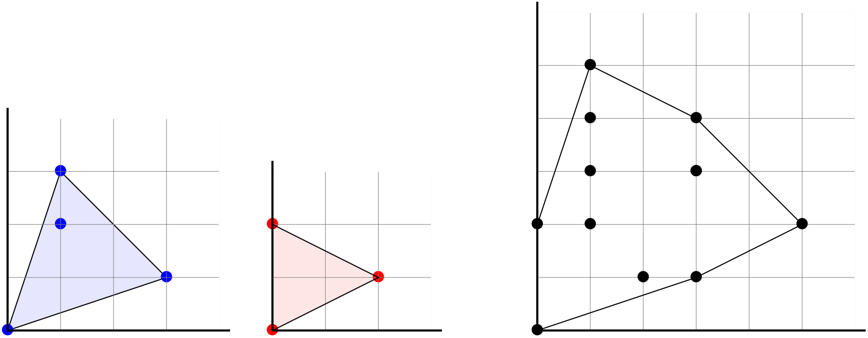
Problem: Let f, g have (at most) t monomials each.
What is the maximal number of vertices of $\mathrm{Newt}(fg+1)$?

An obvious upper bound: $t^2 + 1$.

For $\mathrm{Newt}(fg)$: $2t$ is a tight upper bound.

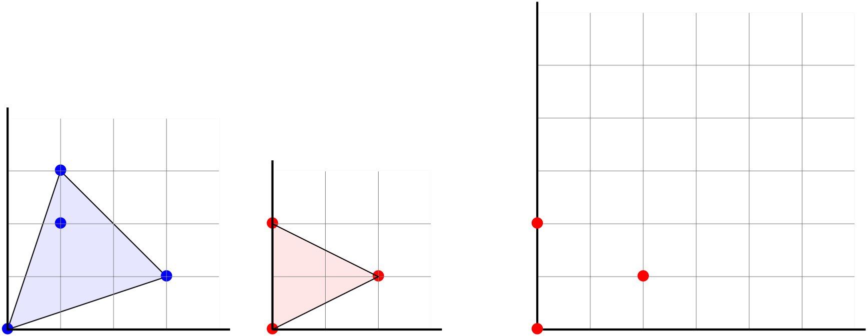
- **Lemma** [Ostrowski] : $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$.
  Minkowski sum: $P + Q = \{p + q, p \in P, q \in Q\}$.
- For convex polygons P, Q with p and q edges,
  the Minkowski sum $P + Q$ has at most $p + q$ edges.
  They are translates of the edges of P and Q.

Connection to Minkowski sums



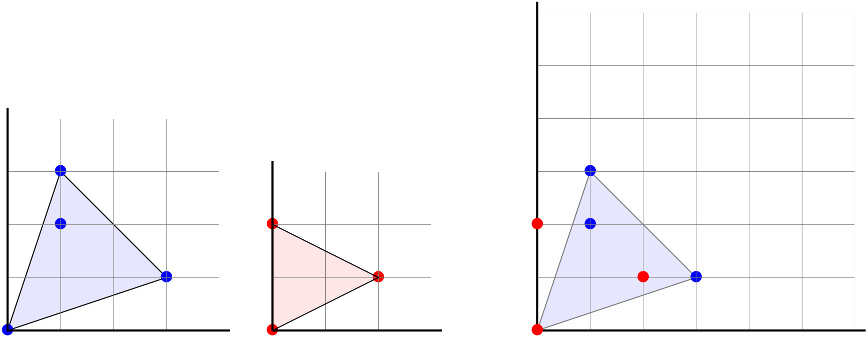
- $f(X,Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X,Y) = 1 + X^2Y + Y^2$
- $(fg)(X,Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



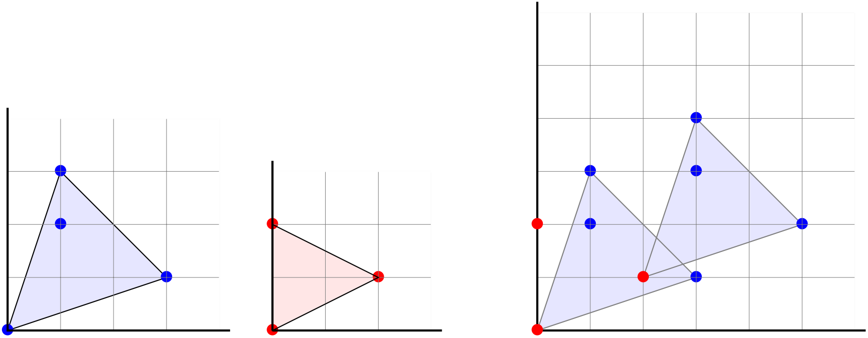
- $f(X,Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X,Y) = 1 + X^2Y + Y^2$
- $(fg)(X,Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



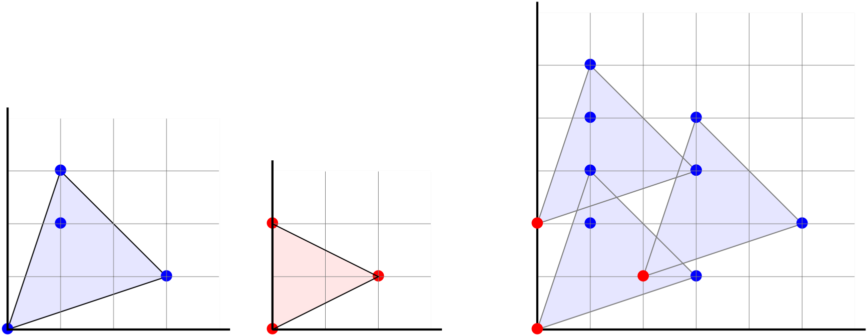
- $f(X, Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X, Y) = 1 + X^2Y + Y^2$
- $(fg)(X, Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



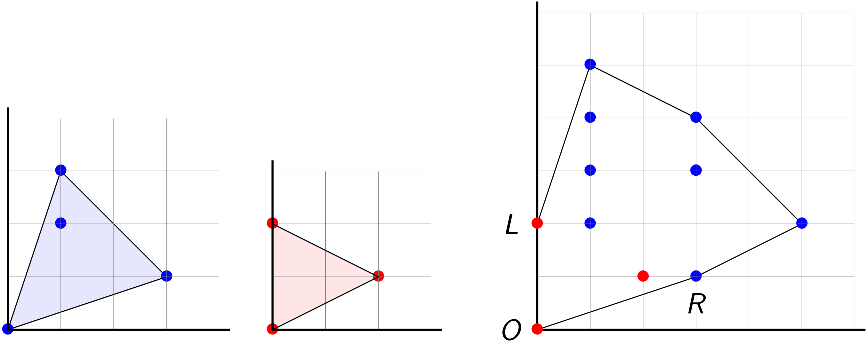
- $f(X,Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X,Y) = 1 + X^2Y + Y^2$
- $(fg)(X,Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



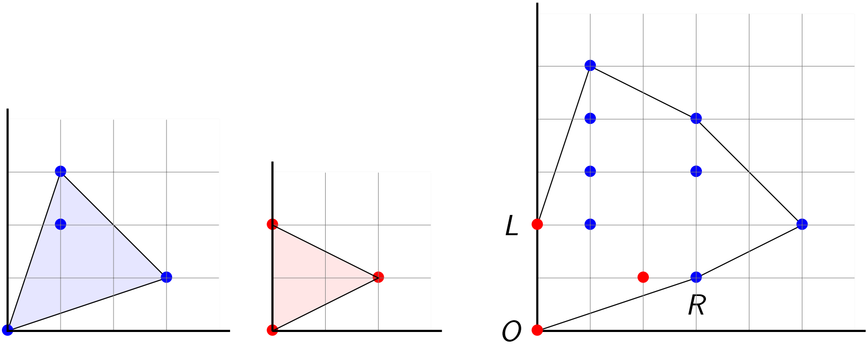
- $f(X, Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X, Y) = 1 + X^2Y + Y^2$
- $(fg)(X, Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



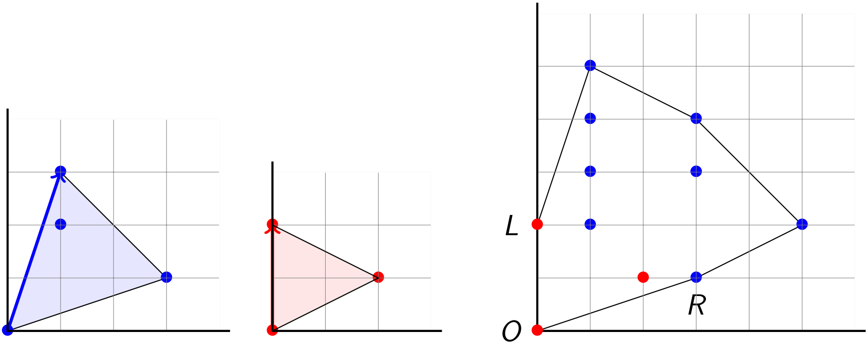
- $f(X,Y) = 1 + X^3Y + XY^2 + XY^3$ et
  $g(X,Y) = 1 + X^2Y + Y^2$
- $(fg)(X,Y) = 1 + Y^2 + XY^2 + XY^3 + XY^4 + XY^5 + X^2Y + X^3Y + 2X^3Y^3 + X^3Y^4 + X^5Y^2$

Connection to Minkowski sums



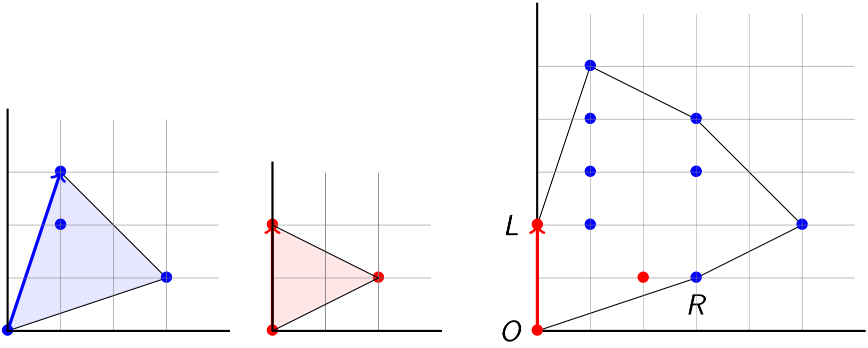
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



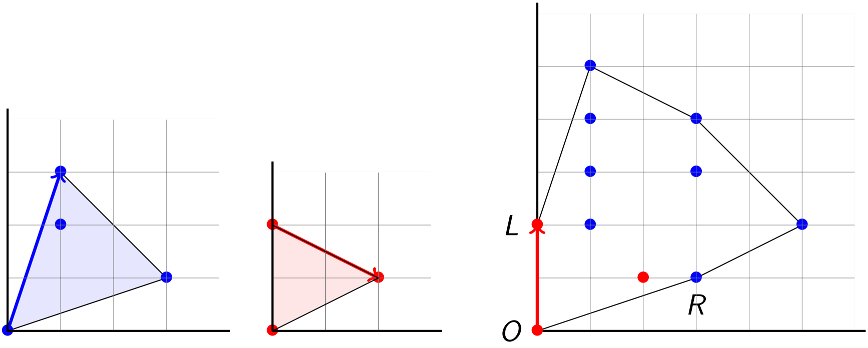
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



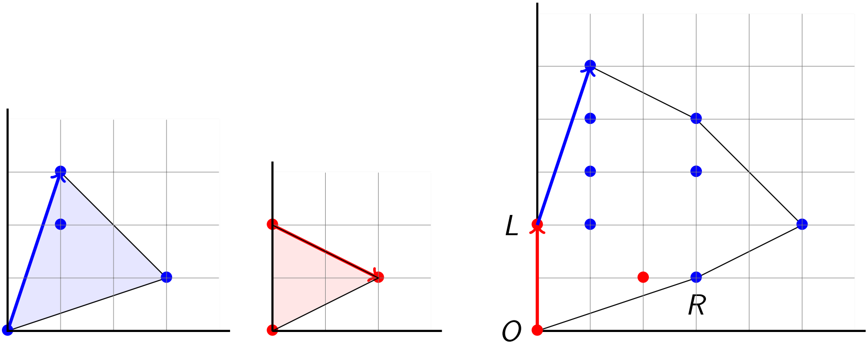
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



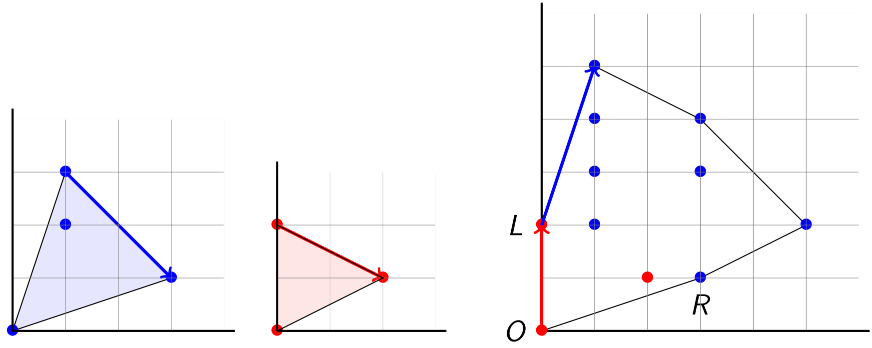
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



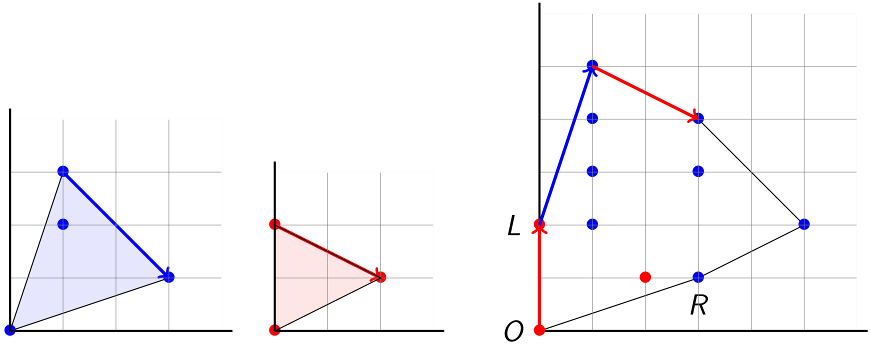
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



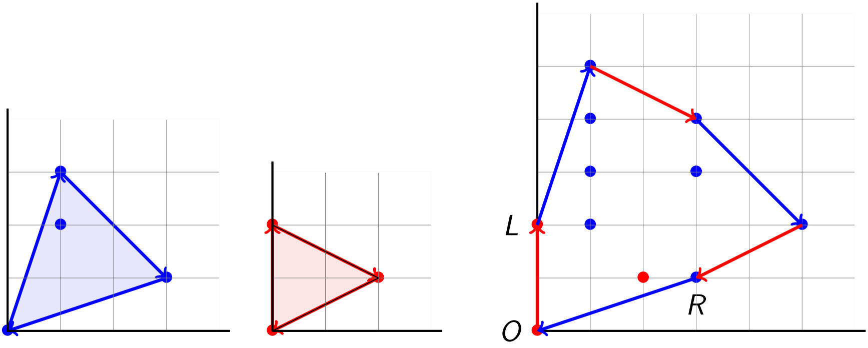
OL has the steepest slope among all edges of P and Q.

Connection to Minkowski sums



OL has the steepest slope among all edges of P and Q.

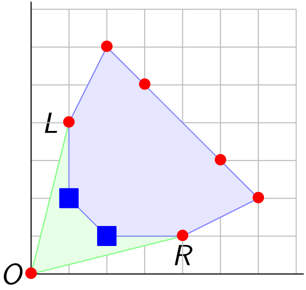
Connection to Minkowski sums



OL has the steepest slope among all edges of P and Q.

The $fg + 1$ problem

- $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$
- If f and g have t monomials, $\mathrm{Newt}(fg)$ has $\leq 2t$ edges.
- For $\mathrm{Newt}(fg + 1)$: cancellations are possible.
- An example: $f(X, Y) = -1 + X^2Y + XY^2$,
  $g(X, Y) = 1 + X^4Y + XY^4$



The trivial bound: t^2

A better bound: $\mathcal{O}(t^{4/3})$

The right bound might be linear...

A complexity theoretic motivation: The τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- Naive upper bound: at most kt^m vertices.
- Conjecture implies VP $\neq$ VNP
  (no polynomial size arithmetic circuits for the permanent).
- Similar problems for univariate polynomials:
  number of real roots, multiplicities of nonzero complex roots.

A complexity theoretic motivation: The τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- Naive upper bound: at most kt^m vertices.
- Conjecture implies VP $\neq$ VNP
(no polynomial size arithmetic circuits for the permanent).
- Similar problems for univariate polynomials:
number of real roots, multiplicities of nonzero complex roots.

A complexity theoretic motivation: The τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- Naive upper bound: at most kt^m vertices.
- Conjecture implies VP $\neq$ VNP
  (no polynomial size arithmetic circuits for the permanent).
- Similar problems for univariate polynomials:
  number of real roots, multiplicities of nonzero complex roots.

The Newton polygon of $fg + 1$: A convexity argument

Consider again the case where fg has constant term -1.

Observation: The vertices of $\mathrm{Newt}(fg + 1)$ form a convexly independent subset of $\mathrm{Mon}(f) + \mathrm{Mon}(g)$.

The Newton polygon of $fg + 1$: A convexity argument

Consider again the case where fg has constant term -1.

Observation: The vertices of $\mathrm{Newt}(fg + 1)$ form
a convexly independent subset of $\mathrm{Mon}(f) + \mathrm{Mon}(g)$.

Theorem [Eisenbrand-Pach-Rothvoß-Sopher'08]:
Let A and B be sets of at most t points each.
Any convexly independent subset of $A + B$ has cardinality $O(t^{4/3})$.

The Newton polygon of $fg + 1$: A convexity argument

Consider again the case where fg has constant term -1.

Observation: The vertices of $\mathrm{Newt}(fg+1)$ form a convexly independent subset of $\mathrm{Mon}(f) + \mathrm{Mon}(g)$.

Theorem [Eisenbrand-Pach-Rothvoß-Sopher'08]:
Let A and B be sets of at most t points each.
Any convexly independent subset of $A + B$ has cardinality $O(t^{4/3})$.

Remark: This bound was shown to be optimal (2010).

The Newton polygon of $fg + 1$: A convexity argument

Consider again the case where fg has constant term -1.

Observation: The vertices of $\mathrm{Newt}(fg + 1)$ form a convexly independent subset of $\mathrm{Mon}(f) + \mathrm{Mon}(g)$.

Theorem [Eisenbrand-Pach-Rothvoß-Sopher'08]:
Let A and B be sets of at most t points each.
Any convexly independent subset of $A + B$ has cardinality $O(t^{4/3})$.

Remark: This bound was shown to be optimal (2010).

Corollary: $\mathrm{Newt}(fg + 1)$ has $O(t^{4/3})$ vertices.

Open problem: Is there a linear upper bound for $fg + 1$?

What if $\mathrm{Mon}(f), \mathrm{Mon}(g)$ are in convex position ?

Students supervised: Karthik C.S. and William Aufort.
Improved result (unpublished): $O(t)$ bound for $\mathrm{Newt}(fg+1)$.

Question: Let A, B be convexly independent sets,
of at most t points each.
Maximal size of a convexly independent subset $S \subseteq A+B$?

Theorem[Tiwary'14]: $|S| = O(t \log t)$.

Remark 1: The right bound in Tiwary's theorem might be $O(t)$.
Remark 2: This question is a generalization of the unit distance problem for sets of points in convex position.

What if $\mathrm{Mon}(f), \mathrm{Mon}(g)$ are in convex position ?

Students supervised: Karthik C.S. and William Aufort.
Improved result (unpublished): $O(t)$ bound for $\mathrm{Newt}(fg+1)$.

Question: Let A, B be convexly independent sets,
of at most t points each.
Maximal size of a convexly independent subset $S \subseteq A + B$?

Theorem[Tiwary'14]: $|S| = O(t \log t)$.

Remark 1: The right bound in Tiwary's theorem might be $O(t)$.
Remark 2: This question is a generalization of the unit distance problem for sets of points in convex position.

What if $\mathrm{Mon}(f), \mathrm{Mon}(g)$ are in convex position ?

Students supervised: Karthik C.S. and William Aufort.
Improved result (unpublished): $O(t)$ bound for $\mathrm{Newt}(fg+1)$.

Question: Let A, B be convexly independent sets,
of at most t points each.
Maximal size of a convexly independent subset $S \subseteq A + B$?

Theorem[Tiwary'14]: $|S| = O(t \log t)$.

Remark 1: The right bound in Tiwary's theorem might be $O(t)$.
Remark 2: This question is a generalization of the unit distance problem for sets of points in convex position.

The unit distance problem

Problem: Let A be a set of t points in the plane.
How many pairs of points p, q of A can be at distance 1?

- Erdös (1946): Slightly superlinear ($t^{1+c/\log\log t}$) lower bound. *Distinct distances* problem appears in the same paper.
- Upper bound: $O(t^{4/3})$ by Spencer-Szemerédi-Trotter (1984).

If A is convex:

- $O(t \log t)$ upper bound by Füredi (1990).
- arxiv preprint by Khopkar (2017) claims $O(t)$ upper bound.

Remark: p, q at distance $1 \Leftrightarrow p - q \in C$ (the unit circle).
Hence: if A contains m pairs at distance 1,
the convex set $A + (-A) \cap C$ has size m.

In particular, Tiwary (2014) reproves Füredi (1990).

The unit distance problem

Problem: Let A be a set of t points in the plane.
How many pairs of points p, q of A can be at distance 1?

- Erdös (1946): Slightly superlinear ($t^{1+c/\log\log t}$) lower bound. *Distinct distances* problem appears in the same paper.
- Upper bound: $O(t^{4/3})$ by Spencer-Szemerédi-Trotter (1984).

If A is convex:

- $O(t \log t)$ upper bound by Füredi (1990).
- arxiv preprint by Khopkar (2017) claims $O(t)$ upper bound.

Remark: p, q at distance $1 \Leftrightarrow p - q \in C$ (the unit circle).
Hence: if A contains m pairs at distance 1,
the convex set $A + (-A) \cap C$ has size m.

In particular, Tiwary (2014) reproves Füredi (1990).

The unit distance problem

Problem: Let A be a set of t points in the plane.
How many pairs of points p, q of A can be at distance 1?

- Erdös (1946): Slightly superlinear ($t^{1+c/\log\log t}$) lower bound.
  Distinct distances problem appears in the same paper.
- Upper bound: $O(t^{4/3})$ by Spencer-Szemerédi-Trotter (1984).

If A is convex:

- $O(t \log t)$ upper bound by Füredi (1990).
- arxiv preprint by Khopkar (2017) claims $O(t)$ upper bound.

Remark: p, q at distance $1 \Leftrightarrow p - q \in C$ (the unit circle).
Hence: if A contains m pairs at distance 1,
the convex set $A + (-A) \cap C$ has size m.

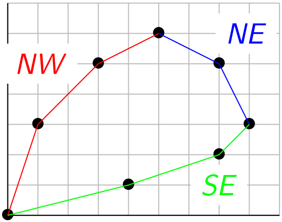
In particular, Tiwary (2014) reproves Füredi (1990).

$S \subseteq A + B$ with A, B, S in convex position: Ingredients of Tiwary's proof

Ingredient 1: $S \subseteq A + A$ with A, S in convex position.

- $|S| \leq 5|A| - 8$ [Halman-Onn-Rothblum'2007].
- Improvement by García-Marco and Knauer (2015): $|S| \leq 2|A| - 2$; an example where $|S| = 3|A|/2$.

Ingredient 2:
Decomposition of a convex polygon A into 4 *convex chains*: $A_{NW}, A_{NE}, A_{SE}, A_{SW}$.

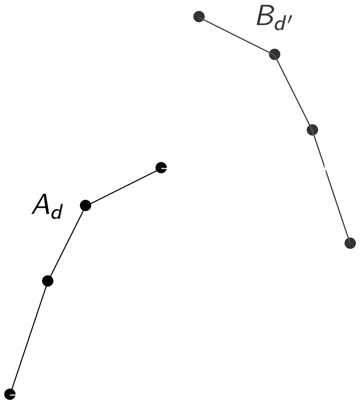


$S \subseteq A + B$: using the two ingredients

We estimate the contribution of $A_d + B_{d'}$ to S for $d, d' \in \{NW, NE, SE, SW\}$.

Lemma: If $d \neq d'$, $|(A_d + B_{d'}) \cap S| \leq 2(|A_d| + |B_{d'}|)$.

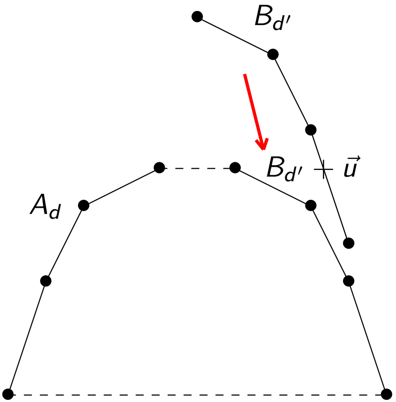
Follows from Argument 1 by translating $B_{d'}$:



$S \subseteq A + B$: using the two ingredients

We estimate the contribution of $A_d + B_{d'}$ to S for $d, d' \in \{NW, NE, SE, SW\}$.
Lemma: If $d \neq d'$, $|(A_d + B_{d'}) \cap S| \leq 2(|A_d| + |B_{d'}|)$.

Follows from Argument 1 by translating $B_{d'}$:



The remaining case: $A_d + B_d$

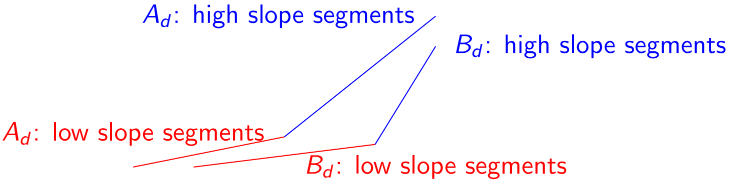
Let $f(n) =$ max size of convexly independent subset of $A_d + B_d$, where $|A_d| + |B_d| \leq n$.

Divide and conquer argument shows:

$$f(n) \leq 2f(n/2) + O(n).$$

Hence $f(n) = O(n \log n)$. $\square$

$f(n) \leq 2f(n/2) + O(n)$ by divide and conquer



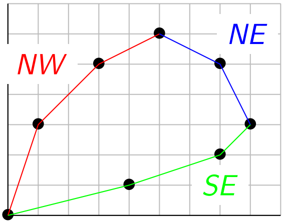
- $|{\color{red}A_d} \cup {\color{red}B_d}| = n/2$, $|{\color{blue}A_d} \cup {\color{blue}B_d}| = n/2$.
- By translation, contributions of ${\color{red}A_d} + {\color{blue}B_d}$, ${\color{red}B_d} + {\color{blue}A_d}$ are $O(n)$.
- Contributions of ${\color{red}A_d} + {\color{red}B_d}$, ${\color{blue}A_d} + {\color{blue}B_d}$ are at most $f(n/2)$.

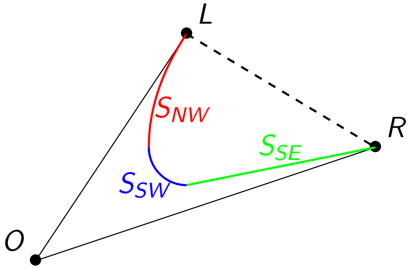
Back to $fg + 1$

- Recall that $A = \mathrm{Mon}(f)$, $B = \mathrm{Mon}(g)$ are in convex position.
- When we remove the origin, new points (S) appear.
- Wanted: bounds on the contributions

$$\left|(A_d + B_{d'}) \cap S_{d''}\right|$$

of the chains of A and B to the chains of S.
- Case $d \neq d'$ already dealt with.





Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

Different Chains

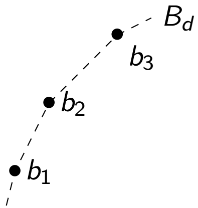
Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

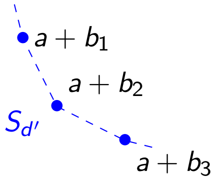


- of type d since $b_i \in B_d$

Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

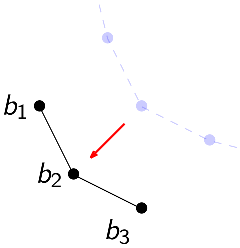


- of type d since $b_i \in B_d$
- of type d' as a translate of a subchain of $S_{d'}$

Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

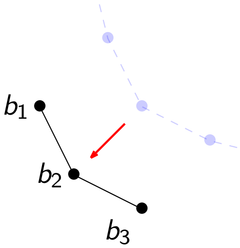


- of type d since $b_i \in B_d$
- of type d' as a translate of a subchain of $S_{d'}$

Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...

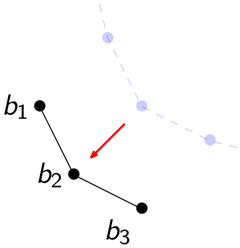


- of type d since $b_i \in B_d$
- of type d' as a translate of a subchain of $S_{d'}$
- Contradiction since $d \neq d'$

Different Chains

Lemma: If $d \neq d'$, $|(A_d + B_d) \cap S_{d'}| \leq |A_d| + |B_d|$.

- Consider the bipartite graph $G = (V, E)$ where $V = A_d \cup B_d$ and $(a, b) \in E \Leftrightarrow a + b \in S_{d'}$
- If a has 3 neighbors b_1, b_2, b_3, they form a chain of type ...



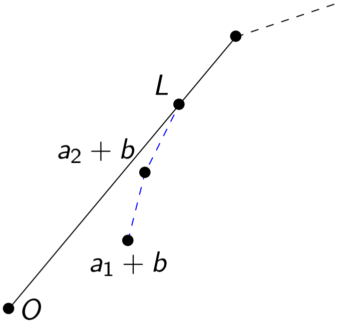
- of type d since $b_i \in B_d$
- of type d' as a translate of a subchain of $S_{d'}$
- Contradiction since $d \neq d'$

- Note: we can replace A_d by A in this proof, even if A is nonconvex.

The slope argument

Lemma

$|(A_d + B) \cap S_d| \leq |B|$ *(B may be nonconvex)*

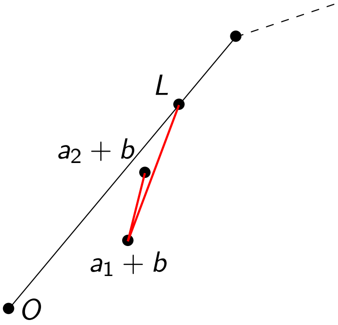


- Consider the same graph G, and $d = NW$.
- If b has 2 neighbors a_1, a_2...

The slope argument

Lemma

$|(A_d + B) \cap S_d| \leq |B|$ *(B may be nonconvex)*

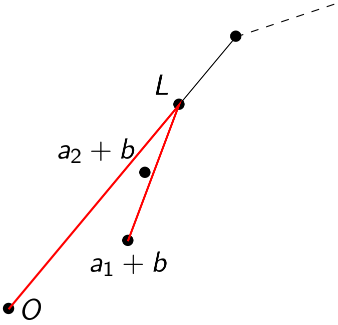


- Consider the same graph G, and $d = NW$.
- If b has 2 neighbors a_1, a_2...
- $\text{slope}(a_1, a_2) >$ $\text{slope}(a_1 + b, L)$

The slope argument

Lemma

$|(A_d + B) \cap S_d| \leq |B|$ *(B may be nonconvex)*

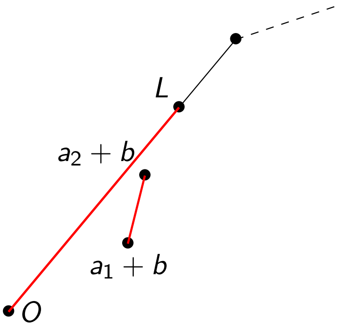


- Consider the same graph G, and $d = NW$.
- If b has 2 neighbors a_1, a_2...
- $\text{slope}(a_1, a_2) > \text{slope}(a_1 + b, L)$
- $\text{slope}(a_1 + b, L) > \text{slope}(O, L)$

The slope argument

Lemma

$|(A_d + B) \cap S_d| \leq |B|$ *(B may be nonconvex)*



- Consider the same graph G, and $d = NW$.
- If b has 2 neighbors a_1, a_2...
- $\text{slope}(a_1, a_2) > \text{slope}(a_1 + b, L)$
- $\text{slope}(a_1 + b, L) > \text{slope}(O, L)$
- $\text{slope}(O, L) \geq \text{slope}\ (a_1, a_2)$ *(OL is the steepest slope in A, B.)*
- Contradiction

What we have shown

Theorem: If Mon(f) and Mon(g) are in convex position, $|\text{Newt}(fg+1)|$ is of linear size.
Extension to:

- $\mathrm{Mon}(f)$ or $\mathrm{Mon}(g)$ nonconvex.
- $\mathrm{Mon}(f)$ and $\mathrm{Mon}(g)$ weakly convex.
- Deletion of several points.

Some open problems

Combinatorial geometry:

(*) Linear bound on $S \subseteq A + A$ with A, S in convex position: what is the right constant?

(**) Unit distance problem for A in convex position.

(***) Maximal size of $S \subseteq A + B$ for A, B, S in convex position.

(****) Unit distance problem (Erdös'46).

Newton polygon of $fg + 1$:

- How to take better care of cancellations?
- Suggestion by Stéphan Thomassé: work with $f, g \in \mathbb{Z}_2[X, Y]$.

Other $fg + 1$ problems:

- Number of real roots of $fg + 1$ with $f, g \in \mathbb{R}[X]$?
- Maximum multiplicity of a nonzero root of $fg + 1$ with $f, g \in \mathbb{C}[X]$?
- Good bounds for more general expressions $\Rightarrow$ VP $\neq$ VNP.

Some open problems

Combinatorial geometry:

(*) Linear bound on $S \subseteq A + A$ with A, S in convex position: what is the right constant?

(**) Unit distance problem for A in convex position.

(***) Maximal size of $S \subseteq A + B$ for A, B, S in convex position.

(****) Unit distance problem (Erdös'46).

Newton polygon of $fg + 1$:

- How to take better care of cancellations?
- Suggestion by Stéphan Thomassé: work with $f, g \in \mathbb{Z}_2[X, Y]$.

Other $fg + 1$ problems:

- Number of real roots of $fg + 1$ with $f, g \in \mathbb{R}[X]$?
- Maximum multiplicity of a nonzero root of $fg + 1$ with $f, g \in \mathbb{C}[X]$?
- Good bounds for more general expressions $\Rightarrow \mathrm{VP} \neq \mathrm{VNP}$.

Some open problems

Combinatorial geometry:

(*) Linear bound on $S \subseteq A + A$ with A, S in convex position: what is the right constant?

(**) Unit distance problem for A in convex position.

(***) Maximal size of $S \subseteq A + B$ for A, B, S in convex position.

(****) Unit distance problem (Erdös'46).

Newton polygon of $fg + 1$:

- How to take better care of cancellations?
- Suggestion by Stéphan Thomassé: work with $f, g \in \mathbb{Z}_2[X, Y]$.

Other $fg + 1$ problems:

- Number of real roots of $fg + 1$ with $f, g \in \mathbb{R}[X]$?
- Maximum multiplicity of a nonzero root of $fg + 1$ with $f, g \in \mathbb{C}[X]$?
- Good bounds for more general expressions $\Rightarrow$ VP $\neq$ VNP.

Onion peeling of Minkowski sums: A new problem of combinatorial geometry?

Onion peeling of a finite set $A \subseteq \mathbb{R}^2$:

1. First layer: compute $\mathrm{conv}(A)$, remove the extremal points.
2. Repeat until $A = \emptyset$.

Onion peeling of a Minkowski sum:
Assume F, G have $\leq t$ points (and are possibly nonconvex).
How many points on k-th layer of $A = F + G$?

Remark: There are at most $2t$ points on first layer.

A result on onion peeling, and a variation

Theorem: k-th layer of $F + G$ is of size $O(kt \log t)$.

A variation: how many points on the convex hull of $(F + G) \setminus H$, if H is of size at most h?

Remark: These questions are relevant to $\mathrm{Newt}(fg - h)$ where f, g, h have positive coefficients.

Appendix

A τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- $k = 1$: $\mathrm{Newt}(f_1 \ldots f_m)$ is the Minkowski sum $\sum_{i=1}^{m} \mathrm{Newt}(f_i)$.
- $k = 2$ is open. What about $\mathrm{Newt}(f_1 \ldots f_m + 1)$?
- Naive upper bound: at most kt^m vertices.
- Improved upper bound: $O(kt^{2m/3})$ by the convexity argument. This argument cannot take us below $t^{m/3}$.

A τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- $k = 1$: $\mathrm{Newt}(f_1 \dots f_m)$ is the Minkowski sum $\sum_{i=1}^{m} \mathrm{Newt}(f_i)$.
- $k = 2$ is open. What about $\mathrm{Newt}(f_1 \dots f_m + 1)$?
- Naive upper bound: at most kt^m vertices.
- Improved upper bound: $O(kt^{2m/3})$ by the convexity argument. This argument cannot take us below $t^{m/3}$.

A τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- $k = 1$: $\mathrm{Newt}(f_1 \dots f_m)$ is the Minkowski sum $\sum_{i=1}^{m} \mathrm{Newt}(f_i)$.
- $k = 2$ is open. What about $\mathrm{Newt}(f_1 \dots f_m + 1)$?
- Naive upper bound: at most kt^m vertices.
- Improved upper bound: $O(kt^{2m/3})$ by the convexity argument. This argument cannot take us below $t^{m/3}$.

A τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- $k = 1$: $\mathrm{Newt}(f_1 \ldots f_m)$ is the Minkowski sum $\sum_{i=1}^{m} \mathrm{Newt}(f_i)$.
- $k = 2$ is open. What about $\mathrm{Newt}(f_1 \ldots f_m + 1)$?
- Naive upper bound: at most kt^m vertices.
- Improved upper bound: $O(kt^{2m/3})$ by the convexity argument. This argument cannot take us below $t^{m/3}$.

A τ-conjecture for Newton polygons

Conjecture: Consider $f \in \mathbb{C}[X, Y]$ of the form

$$f(X, Y) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X, Y)$$

where the f_{ij} have at most t monomials:
The Newton polygon of f has at most $\mathrm{poly}(kmt)$ vertices.
Remarks:

- f is a "sum of products of sparse polynomials."
- $k = 1$: $\mathrm{Newt}(f_1 \dots f_m)$ is the Minkowski sum $\sum_{i=1}^{m} \mathrm{Newt}(f_i)$.
- $k = 2$ is open. What about $\mathrm{Newt}(f_1 \dots f_m + 1)$?
- Naive upper bound: at most kt^m vertices.
- Improved upper bound: $O(kt^{2m/3})$ by the convexity argument. This argument cannot take us below $t^{m/3}$.

The curse of $fg + 1$

Three "toy problems:"

1. Number of vertices for Newton polygon of $fg + 1$:
   trivial bound is $O(t^2)$, best current bound is $O(t^{4/3})$.
2. For real univariate polynomials:
   t monomials $\Rightarrow$ at most $t - 1$ positive real roots (Descartes).
   Number of real roots of $fg + 1$: trivial bound is $O(t^2)$.
3. Any non-zero (complex) root has multiplicity at most $t - 1$ (Hajós lemma).
   Multiplicity of non-zero root of $fg + 1$: trivial bound is $O(t^2)$.

Optimal bound might be $O(t)$ for these 3 problems.
For fg rather than $fg + 1$, an $O(t)$ bound holds true.

The curse of $fg + 1$

Three "toy problems:"

1. Number of vertices for Newton polygon of $fg + 1$:
   trivial bound is $O(t^2)$, best current bound is $O(t^{4/3})$.
2. For real univariate polynomials:
   t monomials $\Rightarrow$ at most $t - 1$ positive real roots (Descartes).
   Number of real roots of $fg + 1$: trivial bound is $O(t^2)$.
3. Any non-zero (complex) root has multiplicity at most $t - 1$ (Hajós lemma).
   Multiplicity of non-zero root of $fg + 1$: trivial bound is $O(t^2)$.

Optimal bound might be $O(t)$ for these 3 problems.
For fg rather than $fg + 1$, an $O(t)$ bound holds true.

The curse of $fg + 1$

Three "toy problems:"

1. Number of vertices for Newton polygon of $fg + 1$:
   trivial bound is $O(t^2)$, best current bound is $O(t^{4/3})$.
2. For real univariate polynomials:
   t monomials $\Rightarrow$ at most $t - 1$ positive real roots (Descartes).
   Number of real roots of $fg + 1$: trivial bound is $O(t^2)$.
3. Any non-zero (complex) root has multiplicity at most $t - 1$ (Hajós lemma).
   Multiplicity of non-zero root of $fg + 1$: trivial bound is $O(t^2)$.

Optimal bound might be $O(t)$ for these 3 problems.
For fg rather than $fg + 1$, an $O(t)$ bound holds true.

The curse of $fg + 1$

Three "toy problems:"

1. Number of vertices for Newton polygon of $fg + 1$:
   trivial bound is $O(t^2)$, best current bound is $O(t^{4/3})$.
2. For real univariate polynomials:
   t monomials $\Rightarrow$ at most $t - 1$ positive real roots (Descartes).
   Number of real roots of $fg + 1$: trivial bound is $O(t^2)$.
3. Any non-zero (complex) root has multiplicity at most $t - 1$ (Hajós lemma).
   Multiplicity of non-zero root of $fg + 1$: trivial bound is $O(t^2)$.

Optimal bound might be $O(t)$ for these 3 problems.
For fg rather than $fg + 1$, an $O(t)$ bound holds true.

Lower bounds from Newton polygons

Theorem:

τ-conjecture for Newton polygons $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent (VP $\neq$ VNP).

Remark: Recall $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$.

Upper bounds of the form $2^{O(m)}(kt)^{O(1)}$,
or even $2^{(m+\log kt)^c}$ for some $c < 2$ are enough.

A Newton polygon with 2^n edges

For $f_n(X, Y) = \sum_{i=1}^{2^n} X^i Y^{i^2}$:

$2^n - 1$ edges on lower hull, 1 edge on upper hull,
since all vertices lie on graph of $i \mapsto i^2$.

Remarks:

- Our preprint's first version uses $g_n(X, Y) = \prod_{i=1}^{2^n} (X + Y^i)$:
  2^n edges on lower hull, 2^n edges on upper hull.
- f_n is very "explicit:" it has 0/1 coefficients
  and they are computable in polynomial time.

Lower bounds from Newton polygons: A proof sketch

1. Assume that the permanent is easy to compute.
2. Express f_n as $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$
   with $k = n^{O(\sqrt{n})}$, $t = n^{O(\sqrt{n})}$, $m = O(\sqrt{n})$.
3. Contradiction with τ-conjecture for Newton polygons: $\mathrm{Newt}(f_n)$ has 2^n vertices.

Main ingredient: Reduction to depth 4 for arithmetic circuits.

No need for results on counting hierarchy by: [Allender, Bürgisser, Kjeldgaard-Pedersen,Miltersen'06, Bürgisser'07].
They are still relevant for the τ-*conjecture for multiplicities* (Hrubes).

Lower bounds from Newton polygons: A proof sketch

1. Assume that the permanent is easy to compute.
2. Express f_n as $\sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$
   with $k = n^{O(\sqrt{n})}$, $t = n^{O(\sqrt{n})}$, $m = O(\sqrt{n})$.
3. Contradiction with τ-conjecture for Newton polygons:
   $\mathrm{Newt}(f_n)$ has 2^n vertices.

Main ingredient: Reduction to depth 4 for arithmetic circuits.

No need for results on counting hierarchy by:
[Allender, Bürgisser, Kjeldgaard-Pedersen,Miltersen'06, Bürgisser'07].
They are still relevant for the τ*-conjecture for multiplicities* (Hrubes).

Reduction to depth 4 [Agrawal-Vinay'08]

Theorem [Tavenas'13]:
Let C be a circuit of size s, degree d, in n variables.
We assume $d, s = n^{O(1)}$.
There is an equivalent depth 4 $(\sum\prod\sum\prod)$ circuit of size $s^{O(\sqrt{d})}$, with multiplication gates of fan-in $O(\sqrt{d})$.

Depth-4 circuit with inputs of the form X^{2^i}, Y^{2^j}, or constants

(Shallow circuit with high-powered inputs)

$\Updownarrow$

Sum of Products of Sparse Polynomials

The $\sum\prod$ gates compute sparse polynomials.

Reduction to depth 4 [Agrawal-Vinay'08]

Theorem [Tavenas'13]:
Let C be a circuit of size s, degree d, in n variables.
We assume $d, s = n^{O(1)}$.
There is an equivalent depth 4 ($\sum \prod \sum \prod$) circuit of size $s^{O(\sqrt{d})}$, with multiplication gates of fan-in $O(\sqrt{d})$.

$$\boxed{\begin{array}{c}\text{Depth-4 circuit with inputs of the form } X^{2^i},\ Y^{2^j}\text{, or constants}\\ \\ \textit{(Shallow circuit with high-powered inputs)}\end{array}}$$

$$\Updownarrow$$

$$\boxed{\text{Sum of Products of Sparse Polynomials}}$$

The $\sum \prod$ gates compute sparse polynomials.

Reduction to depth 4 and Newton polygons: Completing the argument.

Recall $f_n(X, Y) = \sum_{i=1}^{2^n} X^i Y^{i^2}$.

1. Write $f_n(X, Y) = h_n(\overline{X}, \overline{Y})$ where h_n is multilinear in the new variables $X_j = X^{2^j}$, $Y_j = Y^{2^j}$ (consider radix 2 representation of i and i^2).
2. h_n is in VNP by Valiant's criterion, and in VP if VP = VNP.
3. Reduce corresponding circuit for h_n to a depth 4 circuits C_n.
4. Substitute $X_j \mapsto X^{2^j}$, $Y_j \mapsto Y^{2^j}$ in C_n to express f_n as a "small" sum of products of sparse polynomials.

Reduction to depth 4 and Newton polygons: Completing the argument.

Recall $f_n(X, Y) = \sum_{i=1}^{2^n} X^i Y^{i^2}$.

1. Write $f_n(X, Y) = h_n(\overline{X}, \overline{Y})$ where h_n is multilinear in the new variables $X_j = X^{2^j}$, $Y_j = Y^{2^j}$ (consider radix 2 representation of i and i^2).
2. h_n is in VNP by Valiant's criterion, and in VP if VP = VNP.
3. Reduce corresponding circuit for h_n to a depth 4 circuits C_n.
4. Substitute $X_j \mapsto X^{2^j}$, $Y_j \mapsto Y^{2^j}$ in C_n to express f_n as a "small" sum of products of sparse polynomials.

Reduction to depth 4 and Newton polygons: Completing the argument.

Recall $f_n(X,Y) = \sum_{i=1}^{2^n} X^i Y^{i^2}$.

1. Write $f_n(X,Y) = h_n(\overline{X}, \overline{Y})$ where h_n is multilinear in the new variables $X_j = X^{2^j}$, $Y_j = Y^{2^j}$ (consider radix 2 representation of i and i^2).
2. h_n is in VNP by Valiant's criterion, and in VP if VP $=$ VNP.
3. Reduce corresponding circuit for h_n to a depth 4 circuits C_n.
4. Substitute $X_j \mapsto X^{2^j}$, $Y_j \mapsto Y^{2^j}$ in C_n to express f_n as a "small" sum of products of sparse polynomials.

Reduction to depth 4 and Newton polygons: Completing the argument.

Recall $f_n(X, Y) = \sum_{i=1}^{2^n} X^i Y^{i^2}$.

1. Write $f_n(X, Y) = h_n(\overline{X}, \overline{Y})$ where h_n is multilinear in the new variables $X_j = X^{2^j}$, $Y_j = Y^{2^j}$ (consider radix 2 representation of i and i^2).
2. h_n is in VNP by Valiant's criterion, and in VP if VP $=$ VNP.
3. Reduce corresponding circuit for h_n to a depth 4 circuits C_n.
4. Substitute $X_j \mapsto X^{2^j}$, $Y_j \mapsto Y^{2^j}$ in C_n to express f_n as a "small" sum of products of sparse polynomials.

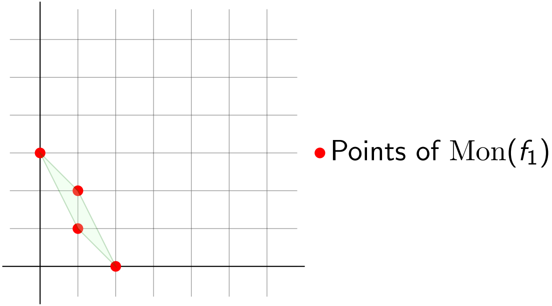
Another Newton polygon, with 2^{n+1} edges

For $f_n(X, Y) = \prod_{i=1}^{2^n}(X + Y^i)$:

2^n edges on lower hull, 2^n edges on upper hull.

The Newton polygon of f_1:

$f_1(X, Y) = (X + Y)(X + Y^2) = X^2 + XY + XY^2 + Y^3$:



The real τ-conjecture

Conjecture: Consider a polynomial $f \in \mathbb{R}[X]$ of the form

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X);$$

where the f_{ij} have at most monomials.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Remarks:

- Case $k = 1$ of the conjecture follows from Descartes' rule (t monomials $\Rightarrow$ at most $2t - 1$ real roots).
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- How many real solutions to $f_1 \dots f_m = 1$?
  How many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The real τ-conjecture

Conjecture: Consider a polynomial $f \in \mathbb{R}[X]$ of the form

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X);$$

where the f_{ij} have at most monomials.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Remarks:

- Case $k = 1$ of the conjecture follows from Descartes' rule (t monomials $\Rightarrow$ at most $2t - 1$ real roots).
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- How many real solutions to $f_1 \ldots f_m = 1$?
  How many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The real τ-conjecture

Conjecture: Consider a polynomial $f \in \mathbb{R}[X]$ of the form

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X);$$

where the f_{ij} have at most monomials.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Remarks:

- Case $k = 1$ of the conjecture follows from Descartes' rule (t monomials $\Rightarrow$ at most $2t - 1$ real roots).
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- How many real solutions to $f_1 \ldots f_m = 1$?
  How many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

The real τ-conjecture

Conjecture: Consider a polynomial $f \in \mathbb{R}[X]$ of the form

$$f(X) = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}(X);$$

where the f_{ij} have at most monomials.
If f is nonzero, its number of **real roots** is polynomial in kmt.
Remarks:

- Case $k = 1$ of the conjecture follows from Descartes' rule (t monomials $\Rightarrow$ at most $2t - 1$ real roots).
- By expanding the products, f has at most $2kt^m - 1$ zeros.
- How many real solutions to $f_1 \dots f_m = 1$?
  How many real solutions to $fg = 1$?
  Descartes' bound is $O(t^2)$ but true bound could be $O(t)$.

Arithmetic circuits:
A model of computation for multivariate polynomials

Shub and Smale's τ-conjecture

$$\begin{aligned}\tau(f) &= \text{size of smallest arithmetic circuit for } f \in \mathbb{Z}[X]\\ &= \text{number of } +, \times \text{ needed to build } f \text{ from } -1, X.\end{aligned}$$

Conjecture:
The number of integer zeros of f is polynomially bounded in $\tau(f)$.

Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow$ $P_{\mathbb{C}} \neq NP_{\mathbb{C}}$.

Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent (Valiant's algebraic version of P versus NP).

Reminder: $\mathrm{per}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}$

Shub and Smale's τ-conjecture

$$\begin{aligned} \tau(f) &= \text{size of smallest arithmetic circuit for } f \in \mathbb{Z}[X] \\ &= \text{number of } +, \times \text{ needed to build } f \text{ from } -1, X. \end{aligned}$$

Conjecture:
The number of integer zeros of f is polynomially bounded in $\tau(f)$.

Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent (Valiant's algebraic version of P versus NP).

Reminder: $\mathrm{per}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}$

Shub and Smale's τ-conjecture

$$\begin{aligned} \tau(f) &= \text{size of smallest arithmetic circuit for } f \in \mathbb{Z}[X] \\ &= \text{number of } +, \times \text{ needed to build } f \text{ from } -1, X. \end{aligned}$$

Conjecture:
The number of integer zeros of f is polynomially bounded in $\tau(f)$.

Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent (Valiant's algebraic version of P versus NP).

Reminder: $\mathrm{per}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}$

Shub and Smale's τ-conjecture

$$\begin{aligned}\tau(f) &= \text{size of smallest arithmetic circuit for } f \in \mathbb{Z}[X] \\ &= \text{number of } +, \times \text{ needed to build } f \text{ from } -1, X.\end{aligned}$$

Conjecture:
The number of integer zeros of f is polynomially bounded in $\tau(f)$.

Theorem [Shub-Smale'95]: τ-conjecture $\Rightarrow$ $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

Theorem [Bürgisser'07]:
τ-conjecture $\Rightarrow$ no polynomial-size arithmetic circuits for the permanent (Valiant's algebraic version of P versus NP).

Reminder: $\operatorname{per}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} X_{i\sigma(i)}$