# A $\tau$-Conjecture for Newton Polygons

Pascal Koiran

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

**December 17, 2015**

# The Newton polygon

Let $f(X, Y) = \sum_{i=1}^{t} a_i X^{\alpha_i} Y^{\beta_i}$, $a_i \neq 0$.

- The monomial set of $f$ is:

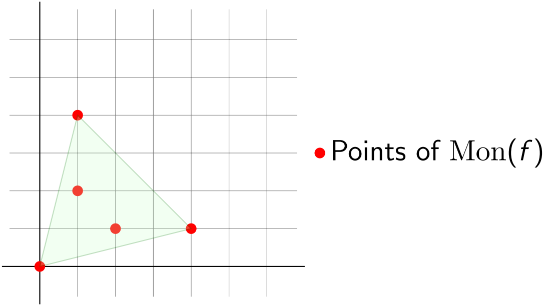
$$\mathrm{Mon}(f) = \{(\alpha_i, \beta_i);\ 1 \leq i \leq t\} \subseteq \mathbb{R}^2.$$

- Its convex hull is the Newton polygon of $f$.

**Abbreviated Notation:**
$f(\mathbb{X}) = \sum_i a_i \mathbb{X}^{f_i}$, where $\mathbb{X} = (X, Y)$, $f_i = (\alpha_i, \beta_i)$.
Thus $\mathrm{Newt}(f) = \mathrm{conv}(\mathrm{Mon}(f)) = \mathrm{conv}(f_i)$.

# A Newton Polygon

$$f(X, Y) = 1 + X^2Y + XY^2 + X^4Y + XY^4.$$



# 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.

- $\mathrm{Newt}(fg)$ is the Minkowski sum of $\mathrm{Newt}(f)$ and $\mathrm{Newt}(g)$.

# 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 $\mathrm{Newt}(fg + 1)$ ?

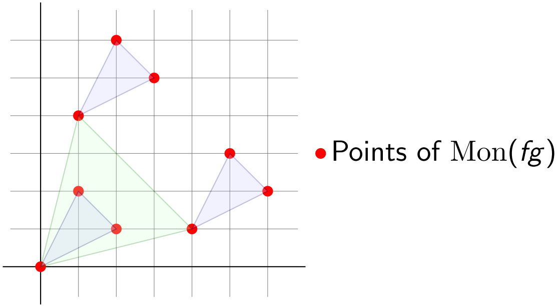
An obvious upper bound: $t^2 + 1$.

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

- $\mathrm{Newt}(fg)$ is the Minkowski sum of $\mathrm{Newt}(f)$ and $\mathrm{Newt}(g)$.
- For convex polygons $P, Q$ with $p$ and $q$ vertices, the Minkowski sum $P + Q$ has at most $p + q$ vertices.

# The Newton polygon of $fg$: an example

$f(X,Y) = 1 + X^2Y + XY^2$ (blue triangle)
$g(X,Y) = 1 + X^4Y + XY^4$ (green triangle)



# The Minkowski sum of convex polygons

**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction; let $P_1$ = leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction; let $Q_1$ = leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_iP_{i+1}$ and $Q_jQ_{j+1}$.

# The Minkowski sum of convex polygons

**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction; let $P_1$ = leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction; let $Q_1$ = leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_iP_{i+1}$ and $Q_jQ_{j+1}$.

# The Minkowski sum of convex polygons

**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction;
   let $P_1 =$ leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction;
   let $Q_1 =$ leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_i P_{i+1}$ and $Q_j Q_{j+1}$.

# The Minkowski sum of convex polygons

**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction;
   let $P_1 =$ leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction;
   let $Q_1 =$ leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_i P_{i+1}$ and $Q_j Q_{j+1}$.

# The Minkowski sum of convex polygons

**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction;
   let $P_1 =$ leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction;
   let $Q_1 =$ leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_i P_{i+1}$ and $Q_j Q_{j+1}$.

# The Minkowski sum of convex polygons

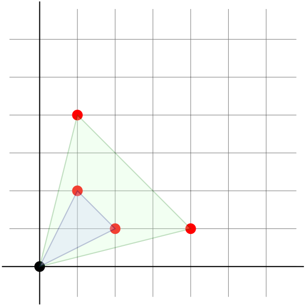
**Definition:** $P + Q = \{x + y;\ x \in P, y \in Q\}$.
$P + Q$ is convex if the sets $P$ and $Q$ are convex.

**Proposition:** For convex polygons, $P + Q = \mathrm{conv}(P_i + Q_j)$ where the $P_i$, $Q_j$ are the vertices of $P$ and $Q$.

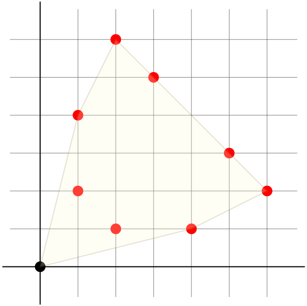
**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction;
   let $P_1$ = leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction;
   let $Q_1$ = leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_iP_{i+1}$ and $Q_jQ_{j+1}$.

# Construction of a Minkowski sum: an example (1/7)

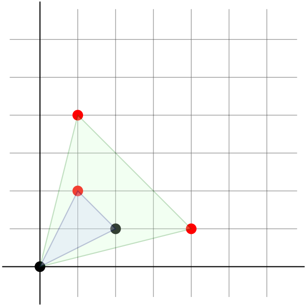


- Initial point for $P$ and $Q$

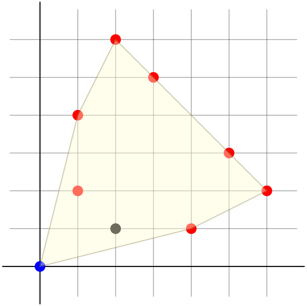


- Initial point for $P + Q$

# Construction of a Minkowski sum: an example (2/7)

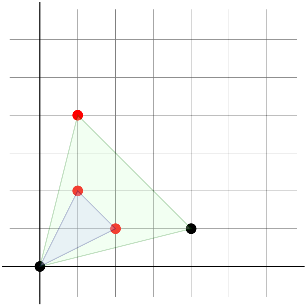


- Potential next points for $P$ and $Q$

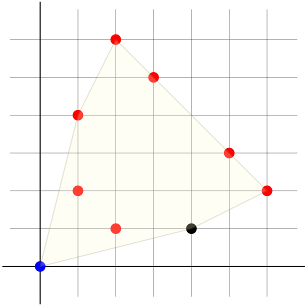


- Potential next point for $P + Q$
- Current point

# Construction of a Minkowski sum: an example (3/7)

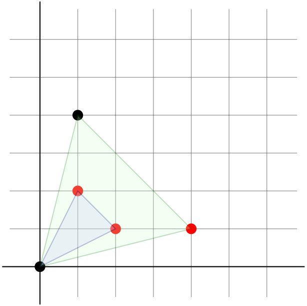


- Next points for $P$ and $Q$

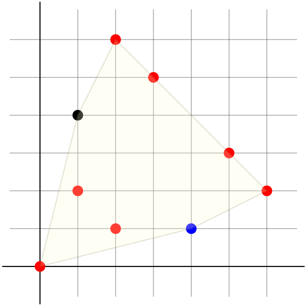


- Next point for $P + Q$
- Current point

# Construction of a Minkowski sum: an example (4/7)

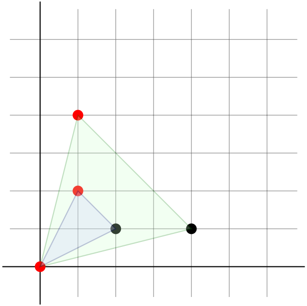


- Potential next points for $P$ and $Q$

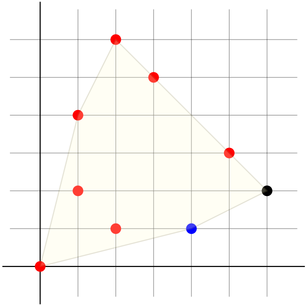


- Potential next point for $P + Q$
- Current point

# Construction of a Minkowski sum: an example (5/7)

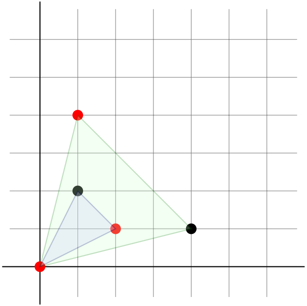


- Next points for $P$ and $Q$

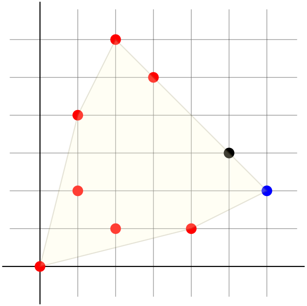


- Next point for $P + Q$
- Current point

# Construction of a Minkowski sum: an example (6/7)

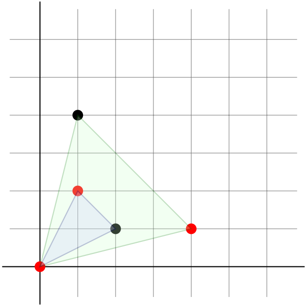


- Potential next points for $P$ and $Q$

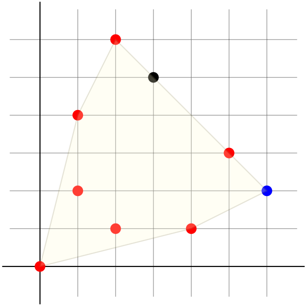


- Potential next point for $P + Q$
- Current point

# Construction of a Minkowski sum: an example (7/7)



- Potential next points for $P$ and $Q$



- Potential next point for $P + Q$
- Current point

# Construction of a Minkowski sum: the analysis

**Incremental construction of $P + Q$:**

1. Order the $P_i$ in counterclockwise direction;
   let $P_1$ = leftmost point of $P$.
2. Order the $Q_j$ in counterclockwise direction;
   let $Q_1$ = leftmost point of $Q$.
3. Leftmost point of $P + Q$ is $P_1 + Q_1$.
4. If current point is $P_i + Q_j$:
   Next point is $P_{i+1} + Q_j$ or $P_i + Q_{j+1}$,
   depending on slopes of $P_iP_{i+1}$ and $Q_jQ_{j+1}$.

**Analysis.** we have constructed $p + q$ points because:

- Pointer $P_i$ may move $p$ times.
- Pointer $Q_j$ may move $q$ times.

# $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$

- $f = \sum_i a_i \mathbb{X}^{f_i}$, $g = \sum_j b_j \mathbb{X}^{g_j}$; $a_i, b_j \neq 0$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i) + \mathrm{conv}(g_j) = \mathrm{conv}(f_i + g_j)$.
- $\mathrm{Newt}(fg) \subseteq \mathrm{Newt}(f) + \mathrm{Newt}(g)$:
  All monomials of $fg$ are of the form $\mathbb{X}^{f_i+g_j}$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$:
  Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$.

Are we done?

# $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$

- $f = \sum_i a_i \mathbb{X}^{f_i}$, $g = \sum_j b_j \mathbb{X}^{g_j}$; $a_i, b_j \neq 0$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i) + \mathrm{conv}(g_j) = \mathrm{conv}(f_i + g_j)$.
- $\mathrm{Newt}(fg) \subseteq \mathrm{Newt}(f) + \mathrm{Newt}(g)$:
  All monomials of $fg$ are of the form $\mathbb{X}^{f_i + g_j}$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$:
  Each monomial $\mathbb{X}^{f_i + g_j}$ appears by expansion of the product $fg$.

Are we done?

# $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$

- $f = \sum_i a_i \mathbb{X}^{f_i}$, $g = \sum_j b_j \mathbb{X}^{g_j}$; $a_i, b_j \neq 0$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i) + \mathrm{conv}(g_j) = \mathrm{conv}(f_i + g_j)$.
- $\mathrm{Newt}(fg) \subseteq \mathrm{Newt}(f) + \mathrm{Newt}(g)$:
  All monomials of $fg$ are of the form $\mathbb{X}^{f_i+g_j}$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$:
  Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$.

Are we done?

# $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$

- $f = \sum_i a_i \mathbb{X}^{f_i}$, $g = \sum_j b_j \mathbb{X}^{g_j}$; $a_i, b_j \neq 0$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i) + \mathrm{conv}(g_j) = \mathrm{conv}(f_i + g_j)$.
- $\mathrm{Newt}(fg) \subseteq \mathrm{Newt}(f) + \mathrm{Newt}(g)$:
  All monomials of $fg$ are of the form $\mathbb{X}^{f_i+g_j}$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$:
  Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$.

Are we done?

# $\mathrm{Newt}(fg) = \mathrm{Newt}(f) + \mathrm{Newt}(g)$

- $f = \sum_i a_i \mathbb{X}^{f_i}$, $g = \sum_j b_j \mathbb{X}^{g_j}$; $a_i, b_j \neq 0$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i) + \mathrm{conv}(g_j) = \mathrm{conv}(f_i + g_j)$.
- $\mathrm{Newt}(fg) \subseteq \mathrm{Newt}(f) + \mathrm{Newt}(g)$:
  All monomials of $fg$ are of the form $\mathbb{X}^{f_i+g_j}$.
- $\mathrm{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$:
  Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$.

Are we done?

# $\mathit{Newt}(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$: a closer look

Recall $\mathit{Newt}(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i + g_j)$.
Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$,
*but it may appear several times.*

**Univariate example:** $(1-X)(1+X+X^2+\cdots+X^n) = 1-X^{n+1}$.

Some observations:

1. $\mathrm{conv}(f_i + g_j)$ is the convex hull of its extremal points.
2. $f_i + g_j$ extremal $\Rightarrow \mathbb{X}^{f_i+g_j}$ appears uniquely in expansion of $fg$:
   If $p = f_i + g_j = f_k + g_l$, then $p = \frac{1}{2}[(f_i + g_l) + (f_k + g_j)]$.
3. If $\mathbb{X}^{f_i+g_j}$ appears uniquely, its coefficient in $fg$ is nonzero.

**Property 2 fails for $fg + 1$.**

## $Newt(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$: a closer look

Recall $Newt(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i + g_j)$.
Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$, *but it may appear several times.*

**Univariate example:** $(1-X)(1+X+X^2+\cdots+X^n) = 1-X^{n+1}$.

Some observations:

1. $\mathrm{conv}(f_i + g_j)$ is the convex hull of its extremal points.
2. $f_i + g_j$ extremal $\Rightarrow \mathbb{X}^{f_i+g_j}$ appears uniquely in expansion of $fg$: If $p = f_i + g_j = f_k + g_l$, then $p = \frac{1}{2}[(f_i+g_l)+(f_k+g_j)]$.
3. If $\mathbb{X}^{f_i+g_j}$ appears uniquely, its coefficient in $fg$ is nonzero.

**Property 2 fails for $fg + 1$.**

# $Newt(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$: a closer look

Recall $Newt(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i + g_j)$.
Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$,
*but it may appear several times.*

**Univariate example:** $(1-X)(1+X+X^2+\cdots+X^n) = 1-X^{n+1}$.

Some observations:

1. $\mathrm{conv}(f_i+g_j)$ is the convex hull of its extremal points.
2. $f_i+g_j$ extremal $\Rightarrow \mathbb{X}^{f_i+g_j}$ appears uniquely in expansion of $fg$:
   If $p = f_i + g_j = f_k + g_l$, then $p = \frac{1}{2}[(f_i+g_l)+(f_k+g_j)]$.
3. If $\mathbb{X}^{f_i+g_j}$ appears uniquely, its coefficient in $fg$ is nonzero.

**Property 2 fails for $fg+1$.**

# $Newt(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$: a closer look

Recall $Newt(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i + g_j)$.
Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$, *but it may appear several times.*

**Univariate example:** $(1-X)(1+X+X^2+\cdots+X^n) = 1-X^{n+1}$.

Some observations:

1. $\mathrm{conv}(f_i + g_j)$ is the convex hull of its extremal points.
2. $f_i + g_j$ extremal $\Rightarrow \mathbb{X}^{f_i+g_j}$ appears uniquely in expansion of $fg$:
   If $p = f_i + g_j = f_k + g_l$, then $p = \frac{1}{2}[(f_i + g_l) + (f_k + g_j)]$.
3. If $\mathbb{X}^{f_i+g_j}$ appears uniquely, its coefficient in $fg$ is nonzero.

**Property 2 fails for $fg + 1$.**

## $Newt(f) + \mathrm{Newt}(g) \subseteq \mathrm{Newt}(fg)$: a closer look

Recall $Newt(f) + \mathrm{Newt}(g) = \mathrm{conv}(f_i + g_j)$.
Each monomial $\mathbb{X}^{f_i+g_j}$ appears by expansion of the product $fg$, *but it may appear several times.*

**Univariate example:** $(1-X)(1+X+X^2+\cdots+X^n) = 1-X^{n+1}$.

Some observations:

1. $\mathrm{conv}(f_i+g_j)$ is the convex hull of its extremal points.
2. $f_i+g_j$ extremal $\Rightarrow \mathbb{X}^{f_i+g_j}$ appears uniquely in expansion of $fg$:
   If $p = f_i + g_j = f_k + g_l$, then $p = \frac{1}{2}[(f_i+g_l)+(f_k+g_j)]$.
3. If $\mathbb{X}^{f_i+g_j}$ appears uniquely, its coefficient in $fg$ is nonzero.

**Property 2 fails for $fg+1$.**

# Back to the Newton polygon of $fg + 1$

Let's compare the monomials of $fg + 1$ and $fg$.

# Back to the Newton polygon of $fg + 1$

Let's compare the monomials of $fg + 1$ and $fg$.

1. If $fg$ has no constant term, $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \cup \{0\}$. Thus $\mathrm{Newt}(fg + 1)$ is the convex hull of $\mathrm{Newt}(fg) \cup \{0\}$: at most $2t + 1$ vertices.

# Back to the Newton polygon of $fg + 1$

Let's compare the monomials of $fg + 1$ and $fg$.

1. If $fg$ has no constant term, $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \cup \{0\}$. Thus $\mathrm{Newt}(fg + 1)$ is the convex hull of $\mathrm{Newt}(fg) \cup \{0\}$: at most $2t + 1$ vertices.
2. If $fg$ and $fg + 1$ both have a constant term: $\mathrm{Newt}(fg + 1) = \mathrm{Newt}(fg)$.

# Back to the Newton polygon of $fg + 1$

Let's compare the monomials of $fg + 1$ and $fg$.

1. If $fg$ has no constant term, $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \cup \{0\}$. Thus $\mathrm{Newt}(fg + 1)$ is the convex hull of $\mathrm{Newt}(fg) \cup \{0\}$: at most $2t + 1$ vertices.
2. If $fg$ and $fg + 1$ both have a constant term: $\mathrm{Newt}(fg + 1) = \mathrm{Newt}(fg)$.
3. If $fg$ has $-1$ as constant term:

# Back to the Newton polygon of $fg + 1$

Let's compare the monomials of $fg + 1$ and $fg$.

1. If $fg$ has no constant term, $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \cup \{0\}$. Thus $\mathrm{Newt}(fg + 1)$ is the convex hull of $\mathrm{Newt}(fg) \cup \{0\}$: at most $2t + 1$ vertices.
2. If $fg$ and $fg + 1$ both have a constant term: $\mathrm{Newt}(fg + 1) = \mathrm{Newt}(fg)$.
3. If $fg$ has $-1$ as constant term: $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \setminus \{0\}$.

# Back to the Newton polygon of $fg + 1$

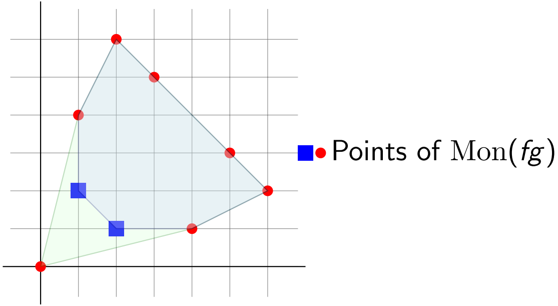
Let's compare the monomials of $fg + 1$ and $fg$.

1. If $fg$ has no constant term, $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \cup \{0\}$.
   Thus $\mathrm{Newt}(fg + 1)$ is the convex hull of $\mathrm{Newt}(fg) \cup \{0\}$:
   at most $2t + 1$ vertices.
2. If $fg$ and $fg + 1$ both have a constant term:
   $\mathrm{Newt}(fg + 1) = \mathrm{Newt}(fg)$.
3. If $fg$ has $-1$ as constant term:
   $\mathrm{Mon}(fg + 1) = \mathrm{Mon}(fg) \setminus \{0\}$.
   The cancellation may expose new points of $\mathrm{Mon}(fg)$!

**Understanding cancellations** seems to be the main difficulty.

# The Newton polygon of $fg - 1$: an example

$f(X,Y) = 1 + X^2Y + XY^2$, $g(X,Y) = 1 + X^4Y + XY^4$.




The 2 blue points lie on the convex hull of $\mathrm{Mon}(fg-1)$, but do not lie on the convex hull of $\mathrm{Mon}(fg)$.

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

Consider again case 3: $fg$ 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 case 3: $fg$ 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 case 3: $fg$ 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 case 3: $fg$ 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 $fg + 1$?
**Remark:** this problem looks very combinatorial if $f, g \in F_2[X, Y]$.

# A $\tau$-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 $\tau$-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 $\tau$-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 $\tau$-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 $\tau$-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 $t^{m/3}$.

# 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.

# Peeling a Minkowski sum
# (A 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:
Let $A = F + G$, where $F$ and $G$ have $t$ points.
How many points on $i$-th layer of $A$ ?
There are at most $2t$ points on first layer.

**Remark:** This is relevant to $\mathrm{Newt}(fg - h)$.

# Peeling a Minkowski sum
# (A 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:
Let $A = F + G$, where $F$ and $G$ have $t$ points.
How many points on $i$-th layer of $A$ ?
There are at most $2t$ points on first layer.

**Remark:** This is relevant to $\mathrm{Newt}(fg - h)$.

# Appendix

# Lower bounds from Newton polygons

**Theorem:**

| | | |
|---|---|---|
| $\tau$-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 $\tau$-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 $\tau$*-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 $\tau$-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 $\tau$-*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 $O(\sqrt{d})$.

| Depth-4 circuit with inputs of the form $X^{2^i}$, $Y^{2^j}$, or constants<br><br>*(Shallow circuit with high-powered inputs)* |
|---|

$\Updownarrow$

| 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.

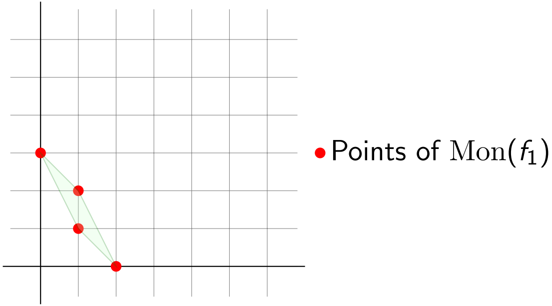
# Another Newton polygon, with $2^{n+1}$ edges

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 $\tau$-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 $\tau$-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 $\tau$-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 $\tau$-conjecture

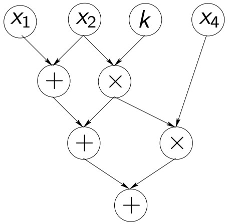
**Conjecture:** Consider a polynomial $f \in \mathbb{R}[X]$ of the form

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

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 $O(t)$.

# Arithmetic circuits:
# A model of computation for multivariate polynomials




Circuit

Size : 9

Depth : 3

# Shub and Smale's $\tau$-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]:** $\tau$-conjecture $\Rightarrow$ $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

**Theorem [Bürgisser'07]:**
$\tau$-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 $\tau$-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]:** $\tau$-conjecture $\Rightarrow \mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

**Theorem [Bürgisser'07]:**
$\tau$-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 $\tau$-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]:** $\tau$-conjecture $\Rightarrow$ $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

**Theorem [Bürgisser'07]:**
$\tau$-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 $\tau$-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]:** $\tau$-conjecture $\Rightarrow$ $\mathrm{P}_{\mathbb{C}} \neq \mathrm{NP}_{\mathbb{C}}$.

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

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