Polynomial Uniqueness via Tournaments

Dave Fetterman

Obviously Unemployed

2/10/23

Abstract

In 2D space, two points $(x_1, y_1), (x_2, y_2), x_1 \neq x_2$ define a line, a polynomial of degree 1. Three distinct points $(x_1, y_1), (x_2, y_2), (x_3, y_3), x_1 \neq x_2 \neq x_3$ define a parabola, a polynomial of degree 2. In general, for finite univariate polynomials of nonnegative, whole degree, $n+1$ such points uniquely specify a polynomial of degree n. Why?

This is the farthest thing from a new result. This is a paper is instead a thoroughly awkward trip through a few mathematical domains to arrive at this well known destination. Helicopters and cars both have their uses. But you wouldn't build a car by turning a helicopter on its side and adding wheels. Metaphorically, I do, so you don't have to.

1 Setup

If we have points $f(x_0) = y_0, f(x_1) = y_1, \ldots f(x_n) = y_n$, how can we determine the coefficients a_i of the polynomial $f(x) = a_0x^0 + a_1x^1 + \ldots + a_nx^n$?

This square matrix of width $n+1$, which I'll denote X_n, is known as a Vandermonde matrix[**1**], and models this set of $n+1$ equations as $X \cdot \vec{a} = \vec{y}$:

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^n \\ 1 & x_1 & x_1^2 & \ldots & x_1^n \\ \vdots & & & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^n \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_n \end{bmatrix}$$

Therefore, we can find our unique coefficient vector A if and only if we can solve $X \cdot \vec{a} = \vec{y}$, or $\vec{a} = X^{-1}\vec{y}$. This has a unique solution if and only if $\det(X) \neq 0$. The rest of this paper tries to find this determinant through all the wrong ways.

2 Finding the Vandermonde determinant

It should be noted that there are other, clearer methods of finding this determinant[**1**] either starting with polynomial unqiueness (basically, going the "other" direction), abstract algebra, direct linear algebra, vector maps, and likely others. These, however, were not the ones I stumbled on.

First, we know that if any $x_i = x_j$ for distinct i, j, we have a zero determinant and no solution. If $f(x_i) = f(x_j), x_i = x_j$, then we are simply underdetermined (not enough points for a unique polynomial). If $f(x_i) = f(x_j), x_i \neq x_j$, then we have an impossible vertical section of our graph. Otherwise, we are in good shape.

This suggests that every pair $(x_i, x_j), i < j$ corresponds to a factor $(x_j - x_i)$ in the determinant, and that the determinant is then some multiple of $D = \prod_{0 \leq i < j \leq n}(x_j - x_i)$.

Taking $n = 2$ as a base case ($n = 1$ produces a boring constant $f(x)$), we see that $\det \begin{bmatrix} 1 & x_0 \\ 1 & x_1 \end{bmatrix} = (x_1 - x_0)$, suggesting D is the determinant of a Vandermonde matrix.

2.1 Setup: Vandermonde inductive step and main theorem

Theorem: The determinant of X_n with generating coefficients $x_0, x_1 ... x_n$ is $\prod_{0 \leq i < j \leq n}(x_j - x_i)$.

With the base case $n = 2$ in hand, the rest of the paper handles the inductive step of proving the main theorem.

Inductive Step of Proof of Theorem:

If, for all X_n, $\det(X_n) = \prod_{0 \leq i < j \leq n}(x_j - x_i)$, then for all $X_{n+1}, \det(X_{n+1}) = \prod_{0 \leq i < j \leq n+1}(x_j - x_i)$.

2.1.1 Definitions

Let's create a few definitions:

- Denote by $M_{n,k}$ the Vandermonde matrix X_n with column n and row k excluded, often called a "matrix minor". *Note: I use zero-indexed matrices in this paper, since in the case of a Vandermonde matrix X_n, the zero-indexed entry (i, j) neatly corresponds to x_i^j.*
- Given an ordered set of indices $I = [0, n]$, denote by P_I the product of all factors the form $(x_j - x_i)$, given $i < j$ and $i, j \in I$. So $P_{[0,2]} = (x_1 - x_0)(x_2 - x_0)(x_2 - x_1)$.

- Given an ordered set of indices $I = [0, n]$, denote by S_I the sum over all permutations σ of I of $sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$. So $S_{[0,2]} = x^2_2x^1_1x^0_0 - x^2_2x^1_0x^0_1 - x^2_1x^1_2x^0_0 + x^2_1x^1_0x^0_2 + x^2_0x^1_2x^0_1 - x^2_0x^1_1x^0_2$.

2.1.2 Proof Plan for Inductive Step

The rest of the proof of the inductive step above follows from showing:

- **P-S Equivalence Lemma**: For a set of indices I, $P_I = S_I$. This is the main statement to prove.
- (1) $det(X_n) = \sum_{k=0}^{n}(-1)^{k+n}x^n_k \det(M_{n,k})$
- (2) For our base base, $\det(X_2) = P_{[0,1]}$
- (3) By inductive hypothesis $det(X_n) = \sum_{k=0}^{n}(-1)^k x^n_k P_{[0,n]-\{k\}}$
- (4) $\sum_{k=0}^{n}(-1)^k x^n_k S_{[0,n]-\{k\}} = S_{[0,n]}$
- (5) By the Lemma, $\sum_{k=0}^{n}(-1)^k x^n_k P_{[0,n]-\{k\}} = P_{[0,n]}$
- (6) Therefore, transitively, $det(X_n) = P_{[0,n]}$.

2.1.3 Straightforward Steps in Proof Plan

(1) is the minor-based definition of the determinant.

The determinant of $X = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ \vdots & & & & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^n \end{bmatrix}$ can be calculated down the rightmost column as

$\det(X) = (-1)^n[x^n_0 \det(M_{n,0}) - x^n_1 \det(M_{n,1}) + ... + (-1)^n x^n \det(M_{n,n})]$.

(2) is clear, with $\det(\begin{bmatrix} 1 & x_0 \\ 1 & x_1 \end{bmatrix}) = -1 \cdot (1 * M_{1,1} - 1 * M_{1,0}) = (x_1 - x_0) = P_{[0,1]}$.

(3) says inductively, we can presuppose that for any $M_{n,k}$, *which is itself a Vandermonde matrix of smaller size*, $\det(M_{n,k})$ can be expressed as $P_{[0,n]-\{k\}}$

(4) This simply splits out all terms of the form $sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$ into those that start with x^n_k and no x_k in the tail, summed over all k. On $\{c, b, a\}$, for example, the terms split out exactly into $c^2(b^1a^0 - b^0a^1) - b^2(c^1a^0 - a^1c^0) + a^2(c^1b^0 - b^1c^0) = c^2b^1a^0 - c^2a^0b^1 - b^2c^1a^0 + b^2a^1c^0 + a^2c^1b^0 - a^2b^1c^0$.

(5) follows from applying the P-S equivalence Lemma to swap instances of S with those of P.

(6) Following the equalities all the way back to 1, $\det(X_n)$ is then $P[0,n]$.

3 Proof of $P_{[0,n]} = S_{[0,n]}$

3.1 Example: $P[0,1] = S[0,1] \Rightarrow P[0,2] = S[0,2]$

We've already established that $P_{[0,1]} = S_{[0,1]}$. To see that $P_{[0,2]} = S_{[0,2]}$, write it out:

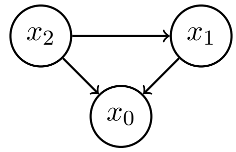
$$\begin{aligned}
& P_{[0,2]} && (1)\\
&= (x_2 - x_1)(x_2 - x_0)P_{[0,1]} && (2)\\
&= (x_2 - x_1)(x_2 - x_0)S_{[0,1]} && (3)\\
&= x_2^2(x_1^1x_0^0 - x_0^1x_1^0) && (4)\\
&+ x_2x_0(x_1^1x_0^0 - x_0^1x_1^0) && (5)\\
&- x_2x_1(x_1^1x_0^0 - x_0^1x_1^0) && (6)\\
&+ x_1x_2(x_1^1x_0^0 - x_0^1x_1^0) && (7)\\
&= x_2^2x_1^1x_0^0 + x_1^2x_0^1x_2^0 + x_0^2x_2^1x_1^0 && (8)\\
&- x_2^2x_0^1x_1^0 - x_1^2x_2^1x_0^0 - x_0^2x_1^1x_2^0 && (9)\\
&+ x_0^1x_1^1x_2^1 - x_0^1x_1^1x_2^1 && (10)\\
&= S_{[0,2]} && (11)
\end{aligned}$$

Note that line (3) follows from line (2) by base case, line (8) is the set of even permutations of $\{2,1,0\}$, line (9) the odds, and line (10) becomes zero.

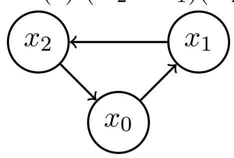
3.2 Graph Intuition

Rather than handle these $2^{\binom{n}{2}}$ terms by hand each time algebraically, we'll treat these factors $(x_j - x_i)$ as a *graph*.

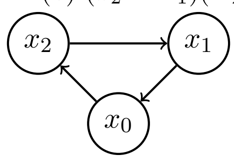
The $2^{\binom{n}{2}} = 2^{\binom{3}{2}} = 8$ terms expanded on lines (8) - (10) are actually the 8 terms resulting from multiplication of the three factors $(x_2 - x_1)(x_2 - x_0)(x_1 - x_0)$. This can be mapped to every possible instance of a complete directed graph (also known as a "tournament")



(a) $(X_2 - x_1)(X_2 - x_0)(X_1 - x_0) = x_2^2 x_1^1 x_0^0$



(b) $(x_2 - X_1)(X_2 - x_0)(x_1 - X_0) = x_2^1 x_1^1 x_0^1$



(c) $(X_2 - x_1)(x_2 - X_0)(X_1 - x_0) = -x_2^1 x_1^1 x_0^1$

Figure 1: Three terms of $P_{[0,2]}$, corresponding to complete directed graphs of size 3

on 3 nodes, with the edge "pointing" from the selected term towards the omitted term in $(x_j - x_i)$.

For example, the term $x_2^2 x_1^1 x_0$, produced by multiplying the left term of the three factors of $(x_2 - x_1)(x_2 - x_0)(x_1 - x_0)$, corresponds to graph 1a. Note we use capital X_1 to mean that term was selected in $(X_1 - x_2)$ for example.

The term $x_2^1 x_1^1 x_0^1$, from multiplying the right, left, and right terms of the above product respectively, corresponds to 1b. And the inverted sequence left, right, left, produces the inverted cycle and algebraic inverse $-x_2^1 x_1^1 x_0^1$ in 1c.

This should give a flavor of the proof.

3.3 P-S Equivalence Lemma Proof layout

Here is a layout of the proof that $P_I = S_I$.

First, we prove a set of lemmas:

- (1) Lemma: The set of terms in an expanded $P_{[0,n]} = \prod_{0 \leq i < j \leq n} (x_j - x_i)$ can be mapped 1:1 to the set of all possible directed complete graphs.
- (2) Lemma :All directed complete graphs are either acyclic or contain a 3-cycle.
- (3) Lemma: Acyclic graphs correspond through the above bijection with terms of the

form $sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$ for some permutation σ on $[0,n]$.

- (4) Lemma: Cyclic tournaments with a 3-cycle can be uniquely paired 1:1 with an otherwise identical graph with that 3-cycle inverted.

Through these lemmas, we can start with a base case equality $P_{[0,2]} = S_{[0,2]}$ and show:

- (5) This bijection maps all possibilities of adding an additional node x_n to an acyclic graph G of $n-1$ nodes to multiplying $\prod_{0 \leq i < n}(x_n - x_i)$ by $P_{[0,n-1]}$
- (6) This bijection maps all possibilities of adding an additional node x_n to an acyclic graph G of $n-1$ nodes to $S_{[0,n]}$.
- (7) Therefore, $P_{[0,n]} = S_{[0,n]}$

3.4 Lemma 1

Every possible complete directed graph $G = (E, V)$ of vertex size n consists exactly of edges $(i \to j)$ with $i, j \in [v_0, v_n - 1], i < j$. If $(i \to j) \in E$, then consider $(X_i - x_j)$ in the expansion of $P_{[0,n-1]}$; otherwise if $(j \to i) \in E$, then consider $(x_i - X_j)$ in the expansion of $P_{[0,n-1]}$. Conversely, if $(X_i - x_j)$ is in a term of $P_{[0,n-1]}$, take $(i \to j)$ for an edge in the graph, otherwise $(j \to i)$. As in Figure 1, this isomorphism should be clear.

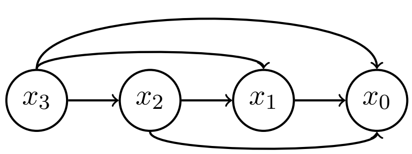
3.5 Lemma 2

If the graph contains no cycles, or a cycle of length 3, we are done.

If a graph contains some cycle $(v_0 \to v_1 \to ... \to v_{m-1} \to v_0)$ of length $m > 3$, we can split it into two possible cycles: $A = (v_0 \to v_1 \to v_2 \to v_0)$ and $B = (v_2 \to v_3 \to ... \to v_0 \to v_2)$. Depending on the direction of edge (v_0, v_2), exactly one of A or B must be a cycle of smaller length. If A is a cycle, we are done. Else use B and reapply recursively, eventually down to a cycle of length 3.

3.6 Lemma 3

Another way of saying "every acyclic tournament maps through some σ to$sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$ is "No acyclic tournament has nodes of equal degree". For example, an acyclic tournament on a set of nodes indexed $[0,3]$ necessarily looks like the following:



Every node has a unique out degree, ranging from $n-1$ to 0. (Note: This graph corresponds to the term $x_3^3 x_2^2 x_1^1 x_0^0$). As every edge "goes right", it's clear that there can be no cycle (or particularly, 3-cycle) here.

For the converse, consider the statement that "no acyclic tournament has a subgraph (removing vertices) with two or more vertices of equal degree". If this is true then certainly the graph has to have the above form out outdegrees. To see this:

- If the graph is of the form $sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$ for some n and some σ, we are done.
- Suppose then it has two vertices with duplicate outdegrees, but has no cycles. Eliminate vertices, starting from x_n, then x_{n-1}, down to x_2 just until a subgraph is of the form with all unique outdegrees, which we'll call $y_m...y_0$, with y_m of outdegree m and y_0 of outdegree 0. Call y_0 for now y^-.
- Add the last removed vertex y^* and its edges back. y^* must have the same outdegree as some other vertex, otherwise we have a contradiction.
- Step: If $(y^- \to y^*)$ is in the graph, then necessarily there is a cycle $(y^- \to y^* \to$ some $y_j \to y^-)$, so we have a contradiction.
- Else $(y^* \to y^-)$ is in the graph, so the outdegree of y^* can't be 0. Remove y^-, reducing all vertices by outdegree 1, creating a new $y^- \neq y^*$ with minimum degree, and go back to (Step).

From this, we can conclude that an acylic directed tournament has vertices of all unique degrees, and thus, up to vertex labeling (permutation), has the form $sgn(\sigma)x^n_{\sigma(n)}x^{n-1}_{\sigma(n-1)}...x^0_{\sigma(0)}$ for some σ.

3.7 Lemma 4

Suppose, for a graph G we fix an ordering of vertices like $\{x_n, x_{n-1}, x_{n-2}...x_0\}$. Suppose (x_a, x_b, x_c) is the 3-cycle with highest lexicographic order $(x_n > x_{n-1} > ...)$, with edges pointing either direction. Then, the graph G', with the same edges, except the direction of cycle (x_a, x_b, x_c) reversed:

- (1) Is a dual to G.
- (2) Has a representation through the main bijection which is an inverse to that of G.

(1) is clear because each uniquely determines the other; the order of vertices is the same, thus the "first" cycle is the same, and the order need only be reversed.
(2) Inverting $(X_1 - x_2)(X_2 - x_3)(X_3 - x_1) = X_1X_2X_3$ yields $(x_1 - X_2)(x_2 - X_3)(x_3 - X_1) = -X_1X_2X_3$, for any choice of x_1, x_2, x_3

4 Pieceyard

Base Case: We've shown this is true for $n = 2 \Rightarrow S_{[0,1]} = (x_1^1 x_0^0 - x_0^1 x_1^0)$. So our inductive step supposes that all terms of (3) for ranges $[0, n-1]$ are of the form $sgn(\sigma)x_{\sigma(n-1)}^{n-1} x_{\sigma(n-2)}^{n-2} ... x_{\sigma(0)}^0$ for some permutation σ on the node set $[0, n-1]$.

The proof that $S_[0,n] = \prod_{0 \leq i < j \leq n} (x_j - x_i)$ requires adding a new node x_n to the left side and a multiplying new set of factors $\prod_{0 \leq i < \leq n} (x_n - x_i)$ by the right side and showing they are equal.

So, for example, we know that $P_{[0,1]} = (x_1 - x_0) = x_1^1 x_0^0 - x_0^1 x_1^0 = S_{[0,1]}$. We can use this to show $P_{[0,2]} = (x_2 - x_1)(x_2 - x_0) P_{[0,1]} = x_2^2 - x_2 x_1 - x_2 x_0$

- Lemma 1: Show an isomorphism between products of the form (3) and tournament graphs on $n+1$ nodes.
- Lemma 2: Show that terms of the form $sgn(\sigma)x_{\sigma(n)}^n x_{\sigma(n-1)}^{n-1} ... x_{\sigma(0)}^0$ remain in (3) after expansion. These correspond to acyclic tournaments on $n+1$ nodes.
- Lemma 3: Show that all other terms in the expansion of (3), which correspond to tournaments with a cycle, can be paired 1:1 with a identical but inverted term, corresponding to an identical graph with *one 3-cycle reversed*.
- Thus, the sum of the terms addressed

5 Prove : VanDerMonde matrix determinant is prod $(x_i - x_j), 1 <= i < j <= n$

This is the determinant of the van der modne matrix

5.1 Base cane: n = 2

5.2 Inductive case

This equalsx^n (product without x), $+y^n$(product without y)...

By inductive hypothesis, each of the terms $x_k^n \det(M_{n,k})$ becomes:

$x_k^n \prod_{0 \leq i < j \leq n; i \neq k, j \neq k} (x_j - x_i)$ or $x_k^n \prod_{0 \leq i < j \leq n; i,j \in I_{n-k}} (x_j - x_i)$

Therefore, we need to prove that $0 \neq \det(X)$

$$= \sum_{k=0}^{n} (-1)^k x_k^n \det(M_{n,k}) \tag{12}$$

$$= \sum_{k=0}^{n} (-1)^k x_k^n \Big[\prod_{0 \le i < j \le n; i,j \in [0,n]-\{k\}} (x_j - x_i) \Big] \tag{13}$$

$$= \prod_{0 \le i < j \le n; i,j \in [0,n]} (x_j - x_i) \tag{14}$$

(1) is a determinant expansion. The *det* term equals the bracketed term of (2) by inductive hypothesis.

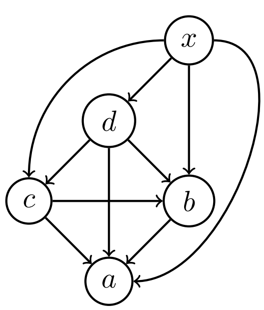
We seek to prove this main theorem:

Theorem: The expansion of (3) is exactly the sum of all possible terms of the form $sgn(\sigma)x_{\sigma(n-1)}^{n-1}x_{\sigma(n-2)}^{n-2}...x_{\sigma(0)}^{0}$ for some permutation σ on the node set $[0, n-1]$. Call this $S_{[0,n]}$. So, for example$S_{\{d,c,b,a\}}$, would be exactly all terms like $d^3c^2b^1a^0$, $-c^3d^2b^1a^0$ or $-c^3a^2d^1b^0$.

If we have this theorem proven, then:

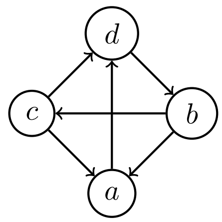
- For $n = 2$, the determinant of X_2 is $1 \cdot x_1 - 1 \cdot x_0 = (x_1^1 x_0^0 - x_0^1 x_1^0) = S_{[0,1]}$
- By inductive hypothesis, the expansion of the bracketed term of (2), $S_{[0,n]-\{k\}}$ yields the same set of sums except each sum excludes all use of x_k.
- The sum of all terms $(-1)^k x_k^n S_{[0,n]-k}$ is exactly $S_{[0,n]}$, meaning (3).
- Therefore, (2) = (3) and we have our Vandermonde determinant (and thus our proof of polynomial uniquenss).

The sorted tournament $d^3c^2b^1a^0$

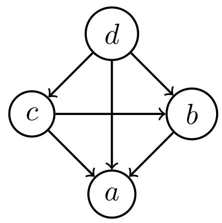


The sorted tournament $x^4d^3c^2b^1a^0$

Factors of $(x-a)(x-b)(x-c)(x-d)$ multiplied by $\sigma = d^3c^2b^1a^0$

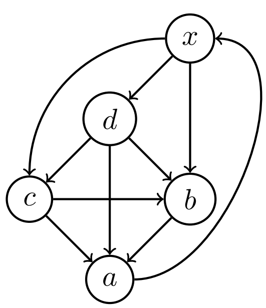


(a) An arbitrary tournament on 4 nodes

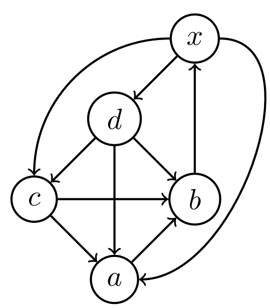


(b) An (acyclic) tournament $d^3c^2b^1a^0$

Figure 2: Tournaments



(a) $-x^3a \cdot d^3c^2b^1a^0$, with cycle (xba)



(b) $-x^3b \cdot -d^3c^2a^1b^0$, with cycle (xab)

Figure 3: Terms in expanded $\prod(x_j - x_i)$ are inverses with inverted 3-cycles

Factor	Product	Matching Factor	Matching σ	Critical pair
x^4	$x^4d^3c^2b^1a^0$	none	none	none
$-x^3a$	$-x^3d^3c^2b^1a^1$	$-x^3b$	$-d^3c^2a^1b^0$	ba
$-x^3b$	$-x^3d^3c^2b^2a^0$	$-x^3c$	$-d^3b^2c^1a^0$	cb
$-x^3c$	$-x^3d^3c^3b^1a^0$	$-x^3d$	$-c^3d^2b^1a^0$	dc
$-x^3d$	$-x^3d^4c^2b^1a^0$	none	none	none
x^2ba	$x^2d^3c^2b^2a^1$	x^2ca	$-d^3b^2c^1a^0$	cb
x^2ca	$x^2d^3c^3b^1a^1$	x^2da	$-c^3d^2b^1a^0$	dc
x^2da	$x^2d^4c^2b^1a^1$	x^2db	$-d^3c^2a^1b^0$	ba
x^2cb	$x^2d^3c^3b^2a^0$	x^2db	$-c^3d^2b^1a^0$	dc
x^2db	$x^2d^4c^2b^2a^0$	x^2dc	$-d^3b^2c^1a^0$	dc
x^2dc	$x^2d^4c^3b^1a^0$	none	none	none
$-xcba$	$-xd^3c^3b^2a^1$	$-xdba$	$-c^3d^2b^1a^0$	dc
$-xdba$	$-xd^4c^2b^2a^1$	$-xcba$	$-d^3b^2c^1a^0$	cb
$-xdca$	$-xd^4c^3b^1a^1$	$-xdcb$	$-d^3c^2a^1b^0$	ba
$-xdcb$	$-xd^4c^3b^2a^0$	none	none	none
$dcba$	$d^4c^3b^2a^1$	none	none	none

6 TODO

6.1 TODO

References

[1] Wikipedia: https://en.wikipedia.org/wiki/Vandermonde_matrix