On the Termination of the General XL Algorithm and Ordinary Multinomials

Gary McGuire* and Daniela Mueller†

School of Mathematics and Statistics
University College Dublin
Ireland

Abstract

The XL algorithm is an algorithm for solving overdetermined systems of multivariate polynomial equations. It was initially introduced for quadratic equations – however the algorithm works for polynomials of any degree and we will focus on the performance of XL for degree $\geq 3$, where the optimal termination value of $D$ is still unknown. We prove that the XL algorithm terminates at a certain value of $D$ when the number of equations exceeds the number of variables by 1 or 2, and give strong evidence that this value is best possible. Our analysis involves some commutative algebra and proving that ordinary multinomials are strongly unimodal, and this result may be of independent interest.

Keywords

XL algorithm, multinomial, ordinary multinomials, unimodal.

*Corresponding Author, gary.mcguire@ucd.ie, Research supported by Science Foundation Ireland Grant 13/IA/1914.
†Research supported by a Postgraduate Government of Ireland Scholarship from the Irish Research Council.
1 Introduction

Algorithms and methods for solving systems of polynomial equations in several variables have many applications, and the XL algorithm is one such method. Most papers so far that analyse the XL algorithm have considered quadratic equations only. In this article we will present some results on the success parameter of the XL algorithm for arbitrary degree polynomials.

In Section 2 we give background on the XL algorithm, and in Section 3 we prove a new theoretical result in commutative algebra (following Diem [Die04]) which will allow us to estimate the optimal termination value.

In Section 4 we will prove that the ordinary multinomials \((N^k)_s\) are strongly unimodal, as well as finding the smallest \(k\) such that the inequality \((N^k)_s \leq k\) holds. These results are of independent interest and this section may be read independently of the rest of the paper. We will prove another inequality involving ordinary multinomials in Section 6. Other papers have outlined proofs of unimodality of ordinary multinomials before; however, our method is different and proves strong unimodality.

Section 5 contains the main results of the paper – our theoretical and computational results on the XL algorithm in the case of one more equation than unknown, and Section 6 considers the case of two more equations than unknowns.

2 Background on the XL algorithm

The XL (eXtended Linearization) Algorithm, introduced in [CKPS00], is an algorithm to solve (overdetermined) systems of multivariate polynomial equations. Consider a system of multivariate polynomial equations

\[
f_1(x_1, \ldots, x_n) = 0
\]

\[
\ldots
\]

\[
f_{n+c}(x_1, \ldots, x_n) = 0
\]

over a (finite) field \(K\), where \(c \geq 1\).

Fix \(D \in \mathbb{N}\), where \(D > \deg(f_i)\) for all \(i\). We call \(D\) the maximal degree. We consider the system of all products

\[
\prod_{l=1}^{k} x_{j_l} \cdot f_i(x_1, \ldots, x_n)
\]
where \( k \leq D - \deg(f_i) \) for \( i = 1, \ldots, n + c \). Note that [CKPS00] assumes \( \deg(f_i) = 2 \) for all \( i \), an assumption we do not make. The idea of the XL algorithm is to linearize this new system in hope of finding a univariate equation which then allows us to solve the initial system.

**Definition 2.1:** (The XL Algorithm)

**Input:** polynomials \( f_1, \ldots, f_{n+c} \) in variables \( x_1, \ldots, x_n \) (an overdetermined system with 0-dimensional solution space) and a positive integer \( D \geq 1 + \max_i \deg(f_i) \).

**Output:** All solutions of the system \( f_1 = 0, \ldots, f_{n+c} = 0 \).

1. **Multiply:** Generate all the products \( \prod_{l=1}^k x_{j_l} \cdot f_i(x_1, \ldots, x_n) \) with \( k \leq D - \deg(f_i) \).

2. **Linearize:** Consider each monomial in the \( x_i \) of degree \( \leq D \) as a new variable and perform Gaussian elimination on the equations obtained in step 1.

   The ordering on the monomials must be such that all the terms containing one (fixed) variable (say \( x_1 \)) are eliminated last.

3. **Solve:** If step 2 yields at least one univariate equation in the powers of \( x_1 \), solve this equation over \( K \). If not, algorithm fails.

4. **Repeat:** Substitute each solution for \( x_1 \) into the other equations and repeat the process to find the values of the other variables.

See [CY04] for some variations and discussions of the algorithm, and a comparison with Gröbner basis algorithms. In particular, it was shown by Moh [Moh00] (see also [CY04]) that the algorithm terminates for some \( D \) provided the solution set is 0-dimensional.

One might set the starting value of \( D \) at \( D = 1 + \max_i \deg(f_i) \). If the ‘Solve’ step fails for this \( D \), or any \( D \), we increment the input value of \( D \) and run the algorithm again. In practice, the first \( D \) at which the algorithm succeeds and terminates is usually larger than \( D = 1 + \max_i \deg(f_i) \).

Considering only those \( D \) for which the XL algorithm succeeds, the algorithm increases in running time with \( D \). Therefore, when looking for maximum efficiency we would like to know the smallest \( D \) such that the XL algorithm succeeds. Let us denote this value by \( D^* \), the optimal input value of \( D \). If we know \( D^* \), we would use this as the starting input value for \( D \). If we don’t know the exact value of \( D^* \) then a lower bound for \( D^* \) is useful.
because we can use the lower bound as the starting value in the XL algorithm. Using ordinary multinomials, we will derive some lower bounds in this article.

3 A Hilbert series associated to the XL algorithm

We will now follow C. Diem (Die04) to set up the theoretical background for determining the optimal choice of the maximal degree $D$.

Let $V_D$ be the $K$-vector space generated by the products produced in the first step of the XL algorithm, i.e.

$$V_D = \left\langle \prod_{i=1}^k x_{j_i} \cdot f_i(x_1, \ldots, x_n) \text{ with } k \leq D - \deg(f_i) \right\rangle_K$$ \hspace{1cm} (1)

Let $K[x_1, \ldots, x_n]_{\leq D}$ be the $K$-vector space of polynomials of total degree $\leq D$. Let

$$\chi(D) := \dim_K(K[x_1, \ldots, x_n]_{\leq D}) - \dim_K(V_D)$$ \hspace{1cm} (2)

**Theorem 3.1:** (Die04) If $\chi(D) \leq D$ then the XL algorithm terminates for that $D$.

**Proof:** Since $\dim_K(K[x_1]_{\leq D}) = D + 1$, if $\chi(D) \leq D$ then $\dim_K(K[x_1]_{\leq D}) > \chi(D)$, i.e. $\dim_K(V_D) + \dim_K(K[x_1]_{\leq D}) > \dim_K(K[x_1, \ldots, x_n]_{\leq D})$ and hence $V_D \cap K[x_1]_{\leq D} \neq \{0\}$. So step 2 of the XL algorithm produces a univariate equation in $x_1$ in this case. \hfill \Box

Clearly then, for reasons of efficiency of the XL algorithm, we would like to know the smallest $D$ such that $\chi(D) \leq D$. We will now try to estimate $\chi(D)$ in order to find the smallest $D$ such that $\chi(D) \leq D$.

Let $K[x_0, x_1, \ldots, x_n]_D$ be the $K$-vector space of all homogeneous polynomials of total degree $D$. Let $F_i \in K[x_0, x_1, \ldots, x_n]$ denote the homogenization of $f_i$. Then $V_D \cong I_D$ via the degree $D$ homogenization map, where

$$I_D := \left\langle \prod_{i=1}^k x_{j_i} \cdot F_i(x_0, x_1, \ldots, x_n) \text{ with } k = D - \deg(F_i) \right\rangle_K$$
Now $I_D$ is the $D^{th}$ homogeneous component of the homogeneous ideal $I := (F_1, \ldots, F_{n+c}) \triangleleft K[x_0, \ldots, x_n]$. It follows that

$$\chi(D) = \dim_K(K[x_0, \ldots, x_n]_D) - \dim_K(I_D)$$

$$= \dim_K(K[x_0, \ldots, x_n]_D/I_D)$$

$$= \dim_K((K[x_0, \ldots, x_n]/I)_D)$$

Definition 3.2: Let $R := K[x_0, \ldots, x_n]$. Let $M = \bigoplus_{i \in \mathbb{N}} M_i$ be a finitely generated positively graded $R$ module. Define the Hilbert function of $M$ as

$$\chi_M : \mathbb{N}_0 \to \mathbb{N}_0$$

$$i \mapsto \dim_R(M_i)$$

and the Hilbert series of $M$ as $H_M := \sum_{i \in \mathbb{N}} \chi_M(i) T^i$.

So $\chi(D) = \chi_{R/I}(D) \forall D \in \mathbb{N}$.

Definition 3.3: (see also [Frö85]) A form $G \in K[x_0, \ldots, x_n]$ of degree $d$ is called generic if all monomials of degree $d$ in $K[x_0, \ldots, x_n]$ have non-zero coefficients in $G$, and those coefficients are algebraically independent over the prime field of $K$.

Lemma 3.4: The Hilbert series of an ideal generated by a generic system of forms depends only on the field characteristic, the rank $n$, and the degrees of the forms. If $\text{char } K = 0$, we call it the generic Hilbert series of type $(n+1; m; d_1, \ldots, d_m)$ where $m$ is the number of forms. (For us, $m = n + c$.)

Proof: See [Die04]. □

Proposition 3.5: Let $K$ be a field (any characteristic), let $F_1, \ldots, F_m \in R := K[x_0, \ldots, x_n]$ be forms of degree $d_1, \ldots, d_m$ (not necessarily generic). Let $I := (F_1, \ldots, F_m) \triangleleft R$. Let $H_g$ be the generic Hilbert series of type $(n+1; m; d_1, \ldots, d_m)$. Then $H_{R/I} \geq H_g$ coefficient-wise.

Proof: See [Die04]. □

Proposition 3.6: Let $G_1, \ldots, G_m = G \in R$ be a generic system of forms with $m \leq n+1$, let $d = \text{deg}(G)$. Let $J := (G_1, \ldots, G_{m-1}) \triangleleft R$. Then for all $D \in \mathbb{N}_0$, the multiplication map

$$G : (R/J)_D \to (R/J)_{D+d}$$

$$\bar{F} \mapsto G \cdot \bar{F}$$

is injective, and we have a short exact sequence

$$0 \to (R/J)_D \xrightarrow{G} (R/J)_{D+d} \to (R/(J,G))_{D+d} \to 0$$
Proposition 3.7: Let \( G_1, \ldots, G_m \in R \) be a generic system of forms of degrees \( d_1, \ldots, d_m \) with \( m \leq n + 1 \). Then
\[
H_{R/(G_1, \ldots, G_m)} = \frac{\prod_{j=1}^{m}(1 - T^{d_j})}{(1 - T)^{n+1}}.
\]

Proof: By the previous proposition, \( H_{(R/J)_{D+a}} = H_{(R/J)_D} + H_{(R/(J,G))_{D+a}} \). The result then follows by induction since \( H_R = \frac{1}{1 - T} \).

All preceding results of this section can be found in [Die04]. We include the statements because they are needed for the next result, which is new.

Theorem 3.8: Let \( F_1, \ldots, F_{n+c} \in R \) (with \( c \geq 1 \)) be forms of degrees \( d_1, \ldots, d_{n+c} \). Then
\[
H_{R/(F_1, \ldots, F_{n+c})} \geq (1 - \sum_{j=n+2}^{n+c} T^{d_j}) \frac{\prod_{j=1}^{n+1}(1 - T^{d_j})}{(1 - T)^{n+1}}
\]
coefficient-wise. If \( d_1 = \ldots = d_{n+c} = d \) then
\[
H_{R/(F_1, \ldots, F_{n+c})} \geq (1 - (c - 1)T^d)(1 + T + \ldots + T^{d-1})^{n+1}
\]
coefficient-wise.

Proof: The case \( d_1 = \ldots = d_{n+c} = 2 \) is done in [Die04]. The general case is similar. We will prove that the generic Hilbert series of type \((n+1; n+c; d_1, \ldots, d_{n+c})\) is \( \geq (1 - \sum_{j=n+2}^{n+c} T^{d_j}) \frac{\prod_{j=1}^{n+1}(1 - T^{d_j})}{(1 - T)^{n+1}} \) coefficient-wise. The result then follows by Proposition 3.7.

Let \( G_1, \ldots, G_{n+c} \in R := K[x_0, \ldots, x_n] \) (with char \( K = 0 \)) be a generic system of forms of degrees \( d_1, \ldots, d_{n+c} \). Let \( R' := R/(G_1, \ldots, G_{n+1}) \) and let \( I' := (G_{n+2}, \ldots, G_{n+c}) \triangleleft R' \). Then \( H_{R'} = \frac{\prod_{j=n+1}^{n+1}(1 - T^{d_j})}{(1 - T)^{n+1}} \) by Proposition 3.7.

Since \( R/(G_1, \ldots, G_{n+c}) \cong R'/I' \),
\[
\chi_{R/(G_1, \ldots, G_{n+c})}(D) = \chi_{R'/I'}(D) = dim_K(R'_D) - dim_K(I'_D).
\]

For \( D \geq d \), \( I'_D = \sum_{j=n+2}^{n+c} G_j \cdot R'_{D-d_j} \) with multiplication map \( G_j : R'_{D-d_j} \rightarrow R'_D \) as in Proposition 3.6. Hence \( dim_K(I'_D) \leq \sum_{j=n+2}^{n+c} dim_K(R'_{D-d_j}) \) by Proposition 3.6. Thus we have
\[
\chi_{R/(G_1, \ldots, G_{n+c})}(D) \geq dim_K(R'_D) - \sum_{j=n+2}^{n+c} dim_K(R'_{D-d_j})
\]
and hence

\[ H_{R/(G_1, \ldots, G_{n+c})} \geq H_{R'} - \sum_{j=n+2}^{n+c} T_{d_j} H_{R'} = \left( 1 - \sum_{j=n+2}^{n+c} T_{d_j} \right) \prod_{j=n+1}^{n+1} (1 - T_{d_j}) \]

\[ \prod_{j=n+1}^{n+1} (1 - T_{d_j}) \]

\[ \square \]

Corollary 3.9: If \( f_1, \ldots, f_{n+1} \in K[x_1, \ldots, x_n] \) (i.e. \( c = 1 \)) with \( \deg(f_i) = d \) for all \( i \), then \( \chi(D) \geq \left( \frac{n+1}{D} \right)_{d-1} \). Furthermore, if all the forms are generic, then equality holds.

**Proof:** Take \( c = 1 \) in Theorem 3.8 and recall that the coefficient of \( T^D \) in \( (1 + T + \ldots + T^d)^{n+1} \) is \( \left( \frac{n+1}{D} \right)_{d-1} \). The second statement follows from Proposition 3.7.

In Section 5 we use this Corollary to find the smallest \( D \) such that \( \chi(D) \leq D \) (and XL succeeds by Theorem 3.1) in the \( c = 1 \) case.

Remark 3.10: We remark that there are three possibly different \( D \)'s under discussion:

1. the smallest \( D \) such that the XL algorithm terminates (call it \( D^* \)),
2. the smallest \( D \) such that \( \chi(D) \leq D \) (call it \( D_\chi \)),
3. the smallest \( D \) such that \( \left( \frac{n+1}{D} \right)_{d-1} \leq D \) (call it \( D_m \)).

**Theorem 3.1** implies that \( D^* \leq D_\chi \). In the case \( c = 1 \), **Corollary 3.9** implies that \( D_m \leq D_\chi \), and \( D_m = D_\chi \) when the equations are generic.

In Section 5 we investigate the relationship between these when \( c = 1 \). At the end of the section we will conjecture that \( D^* = D_\chi = D_m \) when \( c = 1 \) and the equations are generic, and provide evidence.

## 4 Ordinary Multinomials

This section is independent of the rest of the paper. We will prove here that ordinary multinomials are strongly unimodal, and some inequalities.

**Definition 4.1:** A sequence \( s_0, s_1, \ldots, s_N \) of integers is said to be **unimodal** if there is an integer \( t \) with \( 0 \leq t \leq N \) such that

\[ s_0 \leq s_1 \leq \cdots \leq s_t, \quad s_t \geq s_{t+1} \geq \cdots \geq s_N. \]

A unimodal sequence is said to be **strongly unimodal** if all the inequalities are strict, except that \( s_t = s_{t+1} \) may hold. For example, the sequence of binomial coefficients \( \binom{N}{k} \) \((k = 0, 1, \ldots, N)\) is strongly unimodal.

**Remark 4.2:** We remark that there are different definitions of **strongly unimodal** in the literature. One definition is the same as ours except it does not allow \( s_t = s_{t+1} \), in which case the binomial coefficients are strongly unimodal only for \( N \) even.
Definition 4.3: The coefficient of $T^k$ in $(1 + T + \ldots + T^s)^N$ is called **ordinary multinomial** or **generalized binomial coefficient of order** $s$ and is denoted by $\binom{N}{k}_s$.

Combinatorially, $\binom{N}{k}_s$ is the number of different ways of distributing $k$ objects among $N$ boxes, where each box contains at most $s$ objects. See [Bol86] and [Bon93] for an introduction.

$N = 0$: 1  
$N = 1$: 1 1 1 1  
$N = 2$: 1 2 3 4 3 2 1  
$N = 3$: 1 3 6 10 12 12 10 6 3 1  
$N = 4$: 1 4 10 20 31 40 44 40 31 20 10 4 1  

Table 1: Triangle of ordinary multinomials $\binom{N}{k}_s$ with $s = 3$ and $k = 0 \ldots sN$.

Proposition 4.4: (a) $\binom{N}{k}_s = 0$ for $k < 0$ and $k > sN$.

(b) For $s = 1$, the ordinary multinomials are the usual binomial coefficients.

(c) $\binom{N}{k}_s = \sum_{i=0}^{[k/(s+1)]} (-1)^i \binom{N}{i} \binom{k - i(s + 1) + N - 1}{k - i(s + 1)}$

(d) $\binom{N}{k}_s = \sum_{j_1 + \ldots + j_{s+1} = N \atop j_2 + 2j_3 + \ldots + sj_{s+1} = k} \binom{N}{j_1, \ldots, j_{s+1}}$

Proof: (c) follows from expanding $\frac{1 - T^{(s+1)}}{T}^N = \frac{(1-T)^N}{(1-T)^s}$.

(d) follows from the multinomial theorem. □

Lemma 4.5: $\binom{N}{k}_s = \binom{N}{sN-k}_s$, i.e. the ordinary multinomials are symmetric.

Proof: Using Proposition 4.4 (d) if $j_1, \ldots, j_{s+1}$ satisfy $\{j_1 + \ldots + j_{s+1} = N \atop j_2 + 2j_3 + \ldots + sj_{s+1} = k}$, then $j_s + 2j_{s-1} + \ldots + sj_1 = sN - k$ and $\binom{N}{j_1, \ldots, j_{s+1}} = \binom{N}{j_1, \ldots, j_{s+1}}$. □

Lemma 4.6: $\binom{N}{k}_s = \sum_{m=0}^{s} \binom{N-1}{k-m}_s$

Proof: Use Proposition 4.4 (d) and the recurrence relation of multinomial coefficients. □

Theorem 4.7: The ordinary multinomials are strongly unimodal. For $N \geq 2$ we have

$$
\binom{N}{0}_s < \binom{N}{1}_s < \ldots < \binom{\lfloor sN/2 \rfloor}{sN}_s = \binom{\lceil sN/2 \rceil}{sN}_s > \ldots > \binom{N}{sN}_s
$$
Proof: It follows from Lemma 4.6 that

\[
\binom{N}{k+1} = \sum_{m=0}^{s} \binom{N-1}{k+1-m},
\]

\[
= \left(\binom{N-1}{k+1}\right) + \sum_{m=0}^{s} \binom{N-1}{k-m} - \binom{N-1}{k-s}.
\]

So if \(\binom{N-1}{k+1}_s > \binom{N-1}{k-s}_s\) for \(k < \lceil \frac{sN}{2} \rceil\) then \(\binom{N}{k+1}_s > \binom{N}{k}_s\) for \(k < \lceil \frac{sN}{2} \rceil\). We proceed by induction on \(N\).

For \(N = 2\), the base case, \(\binom{1}{k+1}_s > \binom{1}{k-s}_s = 1 - 0 = 1\) for \(0 \leq k < s\). Thus \(\binom{2}{k+1}_s > \binom{2}{k}_s\) for all \(k < \lceil \frac{sN}{2} \rceil\).

Now assume \(\binom{N-1}{k+1}_s > \binom{N-1}{k-s}_s\) for all \(k < \lceil \frac{s(N-1)}{2} \rceil\). Then

\[
\binom{N}{k+1}_s > \binom{N}{k}_s > \cdots > \binom{N}{k-s}_s
\]

whenever \(k < \lceil \frac{s(N-1)}{2} \rceil\). It remains to prove the cases \(\lceil \frac{s(N-1)}{2} \rceil \leq k < \lceil \frac{sN}{2} \rceil\).

If \(k = \lceil \frac{s(N-1)}{2} \rceil + m\) with \(0 \leq m < s/2\) (and hence \(k < \lceil \frac{sN}{2} \rceil\)) then

\[
\binom{N-1}{k+1}_s = \binom{N-1}{s(N-1)-k-1}_s = \binom{N-1}{\lceil \frac{s(N-1)}{2} \rceil - m - 1}_s.
\]

Case 1: where \(s(N-1)\) is even. In this case \(\lceil \frac{s(N-1)}{2} \rceil = \frac{s(N-1)}{2}\) so

\[
\binom{N-1}{k+1}_s = \binom{N-1}{\frac{s(N-1)}{2} - m - 1}_s > \cdots > \binom{N-1}{\frac{s(N-1)}{2} + m - s}_s = \binom{N-1}{k-s}_s
\]

by induction assumption and since \(m < s/2\).

Case 2: where \(s(N-1)\) is odd. In this case \(\lceil \frac{s(N-1)}{2} \rceil = \frac{s(N-1)}{2} + 1\) so

\[
\binom{N-1}{k+1}_s = \binom{N-1}{\frac{s(N-1)}{2} + 1 - m - 1}_s = \binom{N-1}{\frac{s(N-1)}{2} - m}_s
\]

\[
> \cdots > \binom{N-1}{\frac{s(N-1)}{2} + m - s}_s = \binom{N-1}{k-s}_s
\]

by induction assumption and since \(m < s/2\).

Thus, \(\binom{N-1}{k+1}_s > \binom{N-1}{k-s}_s\) and hence \(\binom{N}{k+1}_s > \binom{N}{k}_s\) for all \(k < \lceil \frac{sN}{2} \rceil\).

By symmetry, \(\binom{N}{k+1}_s < \binom{N}{k}_s\) for all \(k \geq \lceil \frac{sN}{2} \rceil\), and \(\binom{N}{\lceil \frac{sN}{2} \rceil}_s = \binom{N}{\lceil \frac{sN}{2} \rceil}_s\). □
Remark 4.8: The smallest mode is given by $\lfloor \frac{sN}{2} \rfloor$. If $sN$ is odd, then we have a plateau of two modes: $\frac{sN-1}{2}$ and $\frac{sN+1}{2}$. If $sN$ is even, then we have a peak at $\frac{sN}{2}$.

Remark 4.9: One can also prove (weak) unimodality of $\binom{N}{k}_s$ using Theorem 4.7 of [DJD88] which says that the convolution of two symmetric discrete unimodal distributions is again unimodal, along with (this relation can be proved using the relation can be proved using $\binom{N}{j_1,\ldots,j_m} = \prod_{i=1}^{m} \binom{\sum_{i=1}^{j_i}}{k}$ and Proposition 4.4 (d)). See also [Bel11].

**Proposition 4.10:** $\binom{N}{k}_s = \binom{N+k-1}{k}$ for $k \leq s$.

*Proof:* $\binom{N+k-1}{k}$ counts the number of ways of putting $k$ objects into $N$ boxes. As noted in [Bon93], $\binom{N}{k}_s$ is the number of ways of putting $k$ objects into $N$ boxes, where each box contains at most $s$ objects.

**Remark 4.11:** By symmetry, if $k \geq s(N-1)$ then $\binom{N}{k}_s = \binom{s+1}{sN-k-1}$. Here is a theorem we will need later in Section 5.

**Theorem 4.12:** For $2 \leq s < \frac{sN}{2} + \frac{2}{N}$, the smallest $k$ such that $\binom{N}{k}_s \leq k$ is $k = sN - 1$.

*Proof:* Claim: $\binom{N}{k}_s > k$ for all $k < \lfloor \frac{sN}{2} \rfloor$.

Proof of claim: $\binom{N}{0}_s = 1 > 0$. Now assume $\binom{N}{k}_s > k$. Then $\binom{N}{k+1}_s \geq \binom{N}{k}_s + 1 > k + 1$ by strong unimodality (Theorem 4.7) for $k < \lfloor \frac{sN}{2} \rfloor$.

Claim: $\binom{N}{k}_s > k$ for all $k \leq sN - 2$ and $2 \leq s < \frac{sN}{2} + \frac{2}{N}$.

Proof of claim: If $\binom{N}{k}_s \leq k$ for some $k \geq \lfloor \frac{sN}{2} \rfloor$, then $\binom{N}{k+1}_s \leq \binom{N}{k}_s + 1 \leq k + 1$ by strong unimodality. By Proposition 4.10, $\binom{N}{sN-2}_s = \binom{N+1}{2} > sN - 2$ for $2 \leq s < \frac{sN}{2} + \frac{2}{N}$.

Again by Proposition 4.10, $\binom{N}{sN-1}_s = \binom{N}{s} = N \leq sN - 1$ for $s \geq 2$. Thus, $k = sN - 1$ is the smallest $k$ such that $\binom{N}{k}_s \leq k$.

**Remark 4.13:** For $s = 1$, the smallest $k$ such that $\binom{N}{k}_1 \leq k$ is $k = N$. If $s \geq \frac{sN}{2} + \frac{2}{N}$, then the smallest $k$ is $sN - 1$. These instances can easily be evaluated directly, see Table 2.

We will also use the following result, which will be proved in Section 6.

**Theorem 4.14:** The smallest $k$ such that $\binom{N}{k}_s - \binom{N}{k-1}_s \leq k$ is

(a) $k = s + 1$ for $N = 2$,

(b) $k = 2s$ for $N = 3$,

(c) $k = \lceil \frac{s(N+1)}{2} \rceil + 1$ for $N \geq 4$. 

10
5 One more equation than unknowns \((c = 1)\) in XL

We are now ready to find our lower bound on the smallest \(D\) such that \(\chi(D) \leq D\) for the case \(c = 1\), i.e., when the number of equations exceeds the number of unknowns by 1. By Theorem 3.1 the XL algorithm will succeed for this \(D\), so this may be a good choice for the initial value of \(D\). We will see that this is actually an excellent choice, and very often the optimal choice.

According to Corollary 3.9, \(\chi(D) \geq \binom{n+1}{D} d^{-1}\) when we have \(n\) unknowns, \(n + 1\) equations, and all equations have the same degree \(d\). According to Theorem 3.1 \(\chi(D) \leq D\) is a sufficient condition for the XL algorithm to succeed. Combining these we get

\[ D \geq \chi(D) \geq \binom{n+1}{D} d^{-1} \]

as sufficient for success, and so we consider the inequality

\[ D \geq \binom{n+1}{D} d^{-1} \]

**Corollary 5.1:** If \(f_1, \ldots, f_{n+1} \in K[x_1, \ldots, x_n]\) with \(\deg(f_i) = d\) for all \(i\) and \(3 \leq d \leq \frac{n+2}{2} + \frac{2}{n+1}\), then the smallest \(D\) such that \(\chi(D) \leq D\) is at least \((d-1)(n+1) - 1\).

**Proof:** Take \(s = d - 1\) and \(N = n + 1\) in Theorem 4.12. \(\Box\)

**Remark 5.2:** This is why we proved Theorem 4.12 earlier. We note that the proof of Theorem 4.12 uses strong unimodality of ordinary multinomials, and this is why we included that result in our paper.

**Remark 5.3:** It follows that for fixed \(d \geq 3\), as \(n\) gets large, the smallest \(D\) such that \(\chi(D) \leq D\) is \(\geq (d-1)(n+1) - 1\). On the other hand, Table 2 gives the value of the smallest \(D\) such that \(\binom{n+1}{D} d^{-1} \leq D\) up to \(d = 10\). Note that this is equal to \((d-1)(n+1) - 1\). Recall from Corollary 3.9 that \(\chi(D) = \binom{n+1}{D} d^{-1}\) when the equations are generic.

**Remark 5.4:** We ran experiments for small values of \(d\) and \(n\), summarised in Table 3. They show that the smallest \(D\) such that \(\chi(D) \leq D\) is equal to the smallest \(D\) such that the XL algorithm terminates, i.e. the lower bound was met in all (but one, see next Remark) of our experiments.
Remark 5.5: In one experiment, namely \( p = 3109, d = 2, n = 6 \), the reader will notice that \( D_{\text{average}} = 6.99 \) and not 7. This means that 1 out of 100 randomly chosen sets of input polynomials finished with \( D = 6 \) and not \( D = 7 \). We then checked this particular set of input polynomials, and two coefficients were equal in one polynomial, i.e., the polynomials were not generic in this one case. This is an example that shows that our bound is (conjecturally) tight for generic polynomials, but non-generic polynomials may finish with a smaller \( D \).

Let us denote by \( D^* \) the optimal input value of \( D \) in the XL algorithm, i.e., \( D^* \) is the smallest \( D \) such that the XL algorithm succeeds. Based on the evidence in Table 3, we conjecture that our lower bound in Corollary 5.1 is tight for generic polynomials.

Conjecture 5.6: When \( c = 1 \) and the polynomials are generic we have \( D^* = (d - 1)(n + 1) - 1 \).

Remark 5.7: In the notation of Remark 3.10, we are conjecturing that \( D^* = D_\chi = D_m \).

Remark 5.8: Our conjecture is consistent with Proposition 6 in [Die04] where it is shown that \( D_\chi \geq n/(1 + \sqrt{c - 1}) \) for quadratic equations. When \( c = 1 \) this becomes \( D_\chi \geq n \), and our conjecture with \( d = 2 \) becomes \( D^* = n \).

Remark 5.9: When the equations do not all have the same degree, we can take \( d \) to be the maximum of the degrees and the above arguments will give a good starting input value for \( D \), but not necessarily the optimal value.

| \( d \) | \( n \) | \( D \) | \( d \) | \( n \) | \( D \) | \( d \) | \( n \) | \( D \) |
|------|------|------|------|------|------|------|------|------|
| 2    | \( \geq 2 \) | \( n + 1 \) | 6    | \( \geq 8 \) | \( 5n + 4 \) | 9    | 2    | \( 8n + 4 \) |
| 3    | \( \geq 2 \) | \( 2n + 1 \) | 7    | 2, 3  | \( 6n + 3 \) | 9    | 3, 4 | \( 8n + 5 \) |
| 4    | 2, 3  | \( 3n + 1 \) | 7    | 4, \ldots, 9 | \( 6n + 4 \) | 9    | 5, \ldots, 13 | \( 8n + 6 \) |
| 4    | \( \geq 4 \) | \( 3n + 2 \) | 7    | \( \geq 10 \) | \( 6n + 5 \) | 9    | \( \geq 14 \) | \( 8n + 7 \) |
| 5    | 2, \ldots, 5 | \( 4n + 2 \) | 8    | 2    | \( 7n + 3 \) | 10   | 2    | \( 9n + 4 \) |
| 5    | \( \geq 6 \) | \( 4n + 3 \) | 8    | 3    | \( 7n + 4 \) | 10   | 3, 4 | \( 9n + 6 \) |
| 6    | 2    | \( 5n + 2 \) | 8    | 4, \ldots, 11 | \( 7n + 5 \) | 10   | 5, \ldots, 15 | \( 9n + 7 \) |
| 6    | 3, \ldots, 7 | \( 5n + 3 \) | 8    | \( \geq 12 \) | \( 7n + 6 \) | 10   | \( \geq 16 \) | \( 9n + 8 \) |

Table 2: The smallest \( D \) such that \( \binom{n+1}{D} \) \( d-1 \leq D \)
Table 3: Running XL on randomly chosen polynomials over prime fields of order \( p \) with one more equation than unknowns. Here \( D_{\text{average}} \) is the average value of the smallest \( D \) such that the XL algorithm terminates over 100 experiments with the same parameters, and \( D_{\text{min}} \) has been calculated according to Table 2. All experiments were done using Magma V2.21-6 [BCP97].

| \( p \) | \( d \) | \( n \) | \( D_{\text{average}} \) | \( D_{\text{min}} \) | \( p \) | \( d \) | \( n \) | \( D_{\text{average}} \) | \( D_{\text{min}} \) |
|------|------|------|-----------------|-------------|------|------|------|-----------------|-------------|
| 3109 | 2    | 2    | 3.00            | 3           | 3109 | 5    | 2    | 10.00           | 10          |
| 5011 | 2    | 2    | 3.00            | 3           | 5011 | 5    | 2    | 10.00           | 10          |
| 3109 | 2    | 3    | 4.00            | 4           | 3109 | 5    | 3    | 14.00           | 14          |
| 5011 | 2    | 3    | 4.00            | 4           | 5011 | 5    | 3    | 14.00           | 14          |
| 3109 | 2    | 4    | 5.00            | 5           | 3109 | 5    | 4    | 18.00           | 18          |
| 5011 | 2    | 4    | 5.00            | 5           | 5011 | 5    | 4    | 18.00           | 18          |
| 3109 | 2    | 5    | 6.00            | 6           | 3109 | 6    | 2    | 12.00           | 12          |
| 5011 | 2    | 5    | 6.00            | 6           | 5011 | 6    | 2    | 12.00           | 12          |
| 3109 | 2    | 6    | 6.99            | 7           | 3109 | 6    | 3    | 18.00           | 18          |
| 5011 | 2    | 6    | 7.00            | 7           | 5011 | 6    | 3    | 18.00           | 18          |
| 3109 | 2    | 7    | 8.00            | 8           | 3109 | 7    | 2    | 15.00           | 15          |
| 5011 | 2    | 7    | 8.00            | 8           | 5011 | 7    | 2    | 15.00           | 15          |
| 3109 | 3    | 2    | 5.00            | 5           | 3109 | 7    | 3    | 21.00           | 21          |
| 5011 | 3    | 2    | 5.00            | 5           | 5011 | 7    | 3    | 21.00           | 21          |
| 3109 | 3    | 3    | 7.00            | 7           | 3109 | 8    | 2    | 17.00           | 17          |
| 5011 | 3    | 3    | 7.00            | 7           | 5011 | 8    | 2    | 17.00           | 17          |
| 3109 | 3    | 4    | 9.00            | 9           | 3109 | 8    | 3    | 25.00           | 25          |
| 5011 | 3    | 4    | 9.00            | 9           | 5011 | 8    | 3    | 25.00           | 25          |
| 3109 | 3    | 5    | 11.00           | 11          | 3109 | 9    | 2    | 20.00           | 20          |
| 5011 | 3    | 5    | 11.00           | 11          | 5011 | 9    | 2    | 20.00           | 20          |
| 3109 | 4    | 2    | 7.00            | 7           | 3109 | 9    | 3    | 29.00           | 29          |
| 5011 | 4    | 2    | 7.00            | 7           | 5011 | 9    | 3    | 29.00           | 29          |
| 3109 | 4    | 3    | 10.00           | 10          | 3109 | 10   | 2    | 22.00           | 22          |
| 5011 | 4    | 3    | 10.00           | 10          | 5011 | 10   | 2    | 22.00           | 22          |
| 3109 | 4    | 4    | 14.00           | 14          | 3109 | 10   | 3    | 33.00           | 33          |
| 5011 | 4    | 4    | 14.00           | 14          | 5011 | 10   | 3    | 33.00           | 33          |
6 Two more equations than unknowns \((c = 2)\) in XL

When \(c > 1\) \((c\) being the difference between the number of equations and the number of unknowns), then [Theorem 3.8] tells us that

\[
\chi(D) \geq \binom{n+1}{D}_{d-1} - (c-1) \binom{n+1}{D-d}_{d-1}
\]

when we have \(n\) unknowns, and all equations have the same degree \(d\). When \(c = 2\) we need the following result.

**Theorem 6.1:** The smallest \(k\) such that \(\binom{N}{k}_{s} - \binom{N}{k-(s+1)}_{s} \leq k\) is

(a) \(k = s + 1\) for \(N = 2\),

(b) \(k = 2s\) for \(N = 3\),

(c) \(k = \lfloor \frac{s(N+1)}{2} \rfloor + 1\) for \(N \geq 4\).

**Proof:**

(a) \(N = 2\): If \(k \leq s\) then \(\binom{2}{k}_{s} \leq \binom{2+k-1}{k} = k + 1\), and thus \(\binom{2}{k}_{s} - \binom{2}{k-(s+1)}_{s} = k + 1 - 0 > k \forall k \leq s\). Now \(\binom{2}{s+1}_{s} \leq \binom{2}{s-1}_{s}\) \(\leq s - 1 \leq s + 1\).

(b) \(N = 3\): If \(k \leq s\) then \(\binom{3}{k}_{s} - \binom{3}{k-(s+1)}_{s} \leq \sum_{m=0}^{k} \binom{2}{k-m}_{s} - \binom{2}{k} > k\) by part (a) and since the ordinary multinomials are...
nonnegative. Now let \( k = s + t \) where \( 1 \leq t \leq s \), i.e. \( s < k \leq 2s \). Thus

\[
\binom{3}{k}_s - \binom{3}{k-(s+1)}_s = \binom{3}{s+t}_s - \binom{3}{t-1}_s
\]

\[\leq\]

\[
\sum_{m=0}^{s} \binom{2}{s+t-m}_s - \sum_{m=0}^{t-1} \binom{2}{t-1-m}_s
\]

\[=\]

\[
\sum_{m=0}^{t-1} \binom{2}{s+t-m}_s + \sum_{m=t}^{s} \binom{2}{s+t-m}_s - \sum_{m=0}^{t-1} \binom{2}{t-1-m}_s
\]

\[=\]

\[
\sum_{m=0}^{t-1} \binom{s-t+m+1}{s-t+m}_s + \sum_{m=t}^{s} \binom{s+t-m+1}{s+t-m}_s - \sum_{m=0}^{t-1} \binom{t-m}{t-1-m}_s
\]

\[=\]

\[
\sum_{m=0}^{t-1} (s-t+m+1) + \sum_{m=t}^{s} (s+t-m+1) - \sum_{m=0}^{t-1} (t-m)
\]

\[=\]

\[
(s-t+1)(s+2t+1) + \frac{t(t-3)}{2} - \frac{s(s+1)}{2}
\]

Now we are left with considering the inequality

\[
(s-t+1)(s+2t+1) + \frac{t(t-3)}{2} - \frac{s(s+1)}{2} > k = s + t
\]

\[
\Leftrightarrow s^2 - 3t^2 + 2st + s - 3t + 2 > 0
\]

Since \( t \leq s \), we can write \( s = t + a \), where \( a \geq 0 \), and substitute:

\[
(t+a)^2 - 3t^2 + 2(t+a)t + (t+a) - 3t + 2 = a^2 + a + 4at - 2t + 2
\]

The right hand side is \( \leq 0 \) when \( a = 0 \), and \( > 0 \) when \( a \geq 1 \). Thus \( \binom{3}{k}_s - \binom{3}{k-(s+1)}_s > k \) whenever \( k < 2s \) and \( \binom{3}{k}_s - \binom{3}{k-(s+1)}_s \leq k \) when \( k = 2s \).

(c) \( N \geq 4 \): Recall that \( \binom{N}{k}_s - \binom{N}{k-1}_s = \binom{N-1}{k}_s - \binom{N-1}{k-(s+1)}_s \) (see proof of Theorem 4.7). We will proceed by induction on \( N \), and assume that \( \binom{N-1}{k}_s - \binom{N-1}{k-(s+1)}_s > k \) for \( k \leq \left\lfloor \frac{sN}{2} \right\rfloor \). Then \( \binom{N}{k}_s - \binom{N}{k-1}_s > k \) and hence \( \binom{N}{k}_s - \binom{N}{k-(s+1)}_s > k \) for \( k \leq \left\lfloor \frac{sN}{2} \right\rfloor \).

For the base case \( N = 4 \), we only have \( \binom{N-1}{k}_s - \binom{N-1}{k-(s+1)}_s > k \) for \( k < \left\lfloor \frac{4N}{2} \right\rfloor \). So we do the case \( k = \left\lfloor \frac{4N}{2} \right\rfloor = 2s \) separately: From the proof of part (b), we have \( \binom{4}{2s}_s - \binom{4}{2s-1}_s = \binom{3}{2s}_s - \binom{3}{2s-(s+1)}_s = 3s + 15 \).
\[
1 + \frac{s(s-3)}{2} - \frac{s(s+1)}{2} = s + 1. \text{ Hence } (\frac{4}{2s})_s - (\frac{4}{s-1})_s = [(\frac{4}{2s})_s - (\frac{4}{s-1})_s] + (\frac{4}{2s-1})_s - (\frac{4}{2s-2})_s + \ldots + [(\frac{4}{s})_s - (\frac{4}{s-4})_s] > s + 1 + \sum_{i=s}^{\infty} i = s + 1 + \frac{(2s-1)(2s)}{2} - \frac{s(s-1)}{2} = s(3s + 1) + 1 > 2s \text{ for } s \geq 1.
\]

Now for \( N \geq 4 \), let \( k = \lfloor \frac{sN}{2} \rfloor + t \), where \( 1 \leq t < \lceil \frac{s}{2} \rceil \). Then

\[
\begin{align*}
\left( \binom{N}{k} \right)_s - \left( \binom{N}{k-(s+1)} \right)_s & \overset{\text{sym.}}{=} \left( \binom{N}{sN-k} \right)_s - \left( \binom{N}{k-(s+1)} \right)_s \\
& = \left( \lfloor \frac{sN}{2} \rfloor - t \right)_s - \left( \lfloor \frac{sN}{2} \rfloor + t - (s+1) \right)_s \\
& = \left( \lfloor \frac{sN}{2} \rfloor - t \right)_s - \left( \lfloor \frac{sN}{2} \rfloor - t - 1 \right)_s + \left( \lfloor \frac{sN}{2} \rfloor - t - 2 \right)_s + \ldots + \left( \lfloor \frac{sN}{2} \rfloor + t - s \right)_s - \left( \lfloor \frac{sN}{2} \rfloor + t - s - 1 \right)_s \\
& > \sum_{i=\lfloor \frac{sN}{2} \rfloor + t-s}^{\lfloor \frac{sN}{2} \rfloor - t} i \text{ (by induction hypothesis)} \\
& = \frac{\lfloor \frac{sN}{2} \rfloor - t)(\lfloor \frac{sN}{2} \rfloor + t + 1) - (\lfloor \frac{sN}{2} \rfloor + t - s)(\lfloor \frac{sN}{2} \rfloor + t - s - 1)}{2} \\
& = \frac{\lfloor \frac{sN}{2} \rfloor^2 - \lfloor \frac{sN}{2} \rfloor + 2s\lfloor \frac{sN}{2} \rfloor + sN - s^2 - s - 2tsN + 2ts}{2} \\
& = \left\{ \begin{array}{ll}
(s^2N + 2sN - s^2 - s - 2tsN + 2ts)/2 & \text{if } 2 \mid sN \\
(s^2N + 2sN - s^2 - s - 2tsN + 2ts)/2 & \text{if } 2 \nmid sN \\
\end{array} \right.
\end{align*}
\]

Case 1: \( 2 \mid sN \). Assume \( 2t \leq s - 1 \).

\[
\frac{s^2N + sN - s^2 - s - 2tsN + 2ts}{2} > \frac{sN}{2} + t \\
\iff s^2N - s^2 - s > 2tsN - 2ts + 2t = 2t(sN - s + 1)
\]

For \( N \geq 4 \), \( 2t \leq s - 1 \) implies

\[
2t(sN - s + 1) \leq s^2N - s^2 - sN + 2s - 1 < s^2N - s^2 - s
\]
**Case 2:** $2 \nmid sN$. Assume $2t \leq s$.

$$\frac{s^2N + 2sN - s^2 - 2s - 2tsN + 2ts}{2} > \frac{sN - 1}{2} + t$$

$$\iff s^2N + sN - s^2 - 2s + 1 > 2tsN - 2ts + 2t = 2t(sN - s + 1)$$

For $N \geq 4$, $2t \leq s$ implies

$$2t(sN - s + 1) \leq s^2N - s^2 + s < s^2N + sN - s^2 - 2s + 1$$

So we have shown \(\binom{N}{k}_s - \binom{N}{k-1}_s > k\) for

$$k \leq \begin{cases} \left\lfloor \frac{s(N+1)}{2} \right\rfloor - 1 & \text{if } 2 \mid s \\ \left\lfloor \frac{s(N+1)}{2} \right\rfloor & \text{if } 2 \nmid s \text{ and } 2 \mid N \\ \left\lfloor \frac{s(N+1)}{2} \right\rfloor - 1 & \text{if } 2 \nmid s \text{ and } 2 \nmid N \end{cases}$$

So we still need to show the case $k = \frac{s(N+1)}{2}$ if $2 \mid s$ and if $2 \nmid sN$.

Assuming that \(\binom{N-1}{k}_s - \binom{N-1}{k-1}_s = \binom{N-2}{k}_s - \binom{N-2}{k-1}_s > k\) for $k \leq \frac{s(N-1)}{2}$ (strong induction), we have

$$\binom{N}{s(N+1)}_s - \binom{N}{s(N-1) + (s+1)}_s \overset{\text{sym.}}{=} \binom{N}{s(N-1)}_s - \binom{N}{s(N-1)}_s - \binom{N}{s(N-1) - 1}_s$$

$$= \binom{N-1}{s(N-1)}_s - \binom{N-1}{s(N-1)}_s - \binom{N-1}{s(N-1) - 1}_s + \ldots$$

$$\binom{N-1}{s(N-1) - s}_s - \binom{N-1}{s(N-1) - s - 1}_s$$

$$> \sum_{i=s(N-1)-s}^{s(N-1)} i = \frac{s^2N + sN - 2s^2 - 2s}{2}$$

$$\overset{?}{>} \frac{s(N+1)}{2} = k$$

The last inequality holds for $N \geq 4$ and $s \geq 2$. The case $s = 1$ corresponds to the usual binomial coefficients and can be shown directly for $N \geq 4$.

For the base case $N = 4$, we only have the weaker assumptions from
parts (a) and (b). But from the proof of part (b) we have
\[
\left(\frac{4}{s} - \frac{4}{s + 1}\right)_{s} = \left(\frac{3}{s} - \frac{3}{s + 1}\right)_{s}
\]
\[
= (\frac{s}{2} + 1)(2s + 1) + \frac{s(s + 1)}{2} > \frac{5s}{2} \text{ for all } s.
\]
Also, for the case \(N = 5\), we only have \(\left(\frac{4}{2s}\right)_{s} - \left(\frac{4}{2s-1}\right)_{s} = s + 1\). So we
have \(\left(\frac{5}{3s}\right)_{s} - \left(\frac{5}{3s-(s+1)}\right)_{s} = \ldots > s + 1 + \sum_{i=s}^{2s-1} i = \frac{s(3s + 1)}{2} + 1 > 3s\) for
\(s \geq 2\). For \(s = 1\), \(\left(\frac{5}{3}\right) - \left(\frac{5}{1}\right) = 5 > 3\).

Now if \(k = \left\lfloor \frac{s(N+1)}{2} \right\rfloor + 1\) then
\[
\left(\frac{N}{\left\lfloor \frac{s(N+1)}{2} \right\rfloor + 1}\right)_{s} - \left(\frac{N}{\left\lfloor \frac{s(N+1)}{2} \right\rfloor + 1 - (s + 1)}\right)_{s}
\]
\[
= \left(\frac{N}{\left\lfloor \frac{s(N-1)}{2} \right\rfloor - 1}\right)_{s} - \left(\frac{N}{\left\lfloor \frac{s(N-1)}{2} \right\rfloor}\right)_{s} \leq 0 \leq k
\]

Thus \(k = \left\lfloor \frac{s(N+1)}{2} \right\rfloor + 1\) is the smallest \(k\) such that \(\binom{N}{k}_{s} - \binom{N}{(k-(s+1))}_{s} \leq k\).

\(\square\)

**Corollary 6.2:** (\(c = 2\)) If \(f_1, \ldots, f_{n+2} \in K[x_1, \ldots, x_n]\) with \(\deg(f_i) = d\)
\(\forall i = 1, \ldots, n + 2\), then the smallest \(D\) such that \(\chi(D) \leq D\) is

(a) \(\geq 2(d - 1)\) for \(n = 2\),

(b) \(\geq \left\lfloor \frac{(d-1)(n+2)}{2} \right\rfloor + 1\) for \(n \geq 3\).

We conjecture that this lower bound is tight.

Based on the \(c = 1\) and \(c = 2\) cases, it appears as though the optimal
starting value for \(D\) in the XL algorithm will be approximately \((d-1)(n+c)/c\).

**References**

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma
algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory
(London, 1993).
[Bel11] Hacène Belbachir. Determining the mode for convolution power of discrete uniform distribution. *Probability in the Engineering and Informational Sciences*, 25:469 – 475, 2011.

[Bol86] Richard C. Bollinger. A note on pascal T-triangles, multinomial coefficients and pascal pyramids. *The Fibonacci Quarterly*, 24(2):140–144, 1986.

[Bon93] Boris A. Bondarenko. *Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs, and Applications*. Fibonacci Association, 1993.

[CKPS00] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, pages 392–407, 2000.

[CY04] Jiun-Ming Chen and Bo-Yin Yang. All in the XL family: Theory and practice. In *Information Security and Cryptology - ICISC 2004, 7th International Conference, Seoul, Korea, December 2-3, 2004, Revised Selected Papers*, pages 67–86, 2004.

[Die04] Claus Diem. The XL-algorithm and a conjecture from commutative algebra. In *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, pages 323–337, 2004.

[DJD88] Sudhakar Dharmadhikari and Kumar Joag-Dev. *Unimodality, Convexity, and Applications*. Academic Press, 1988.

[Frö85] Ralf Fröberg. An inequality for hilbert series of graded algebras. *Journal of Symbolic Computation*, 56(2):117–144, 1985.

[Moh00] T. Moh. On the method of ”xl” and its inefficiency to ttm. *https://eprint.iacr.org/2001/047*, 2000.