Reconstruction problems for graphs, Krawtchouk polynomials and Diophantine equations

Thomas Stoll

June 11, 2008

Abstract

We give an overview about some reconstruction problems in graph theory, which are intimately related to integer roots of Krawtchouk polynomials. In this context, Tichy and the author recently showed that a binary Diophantine equation for Krawtchouk polynomials only has finitely many integral solution. Here, this result is extended. By using a method of Krasikov, we decide the general finiteness problem for binary Krawtchouk polynomials within certain ranges of the parameters.

1 Introduction

1.1 The Reconstruction Conjecture

A famous conjecture in graph theory states that graphs are determined (up to isomorphism) by their subgraphs. This conjecture is known as the *(Kelly-Ulam-) Reconstruction Conjecture* and the literature on solving the conjecture for special graphs is vast (see [2] for a survey). Also, negative results are known, for example, digraphs and hypergraphs are in general not *reconstructible*. On the other hand, there is much freedom in formulating reconstructions problems, namely, one may remove edges, vertices or specific sets of vertices for the subgraphs under question. The aim of the present chapter is to give a short overview on how these reconstruction problems relate to the investigation of integral zeroes of so-called *Krawtchouk polynomials* as well as to report on known results on this connection. Indeed, reconstruction can be put in terms of a one-variable Diophantine problem for Krawtchouk polynomials. It is a great challenge to study this Diophantine problem in the most general setting, hereby making a substantial attempt to unify several of the dispersed results in the area of graph reconstruction.

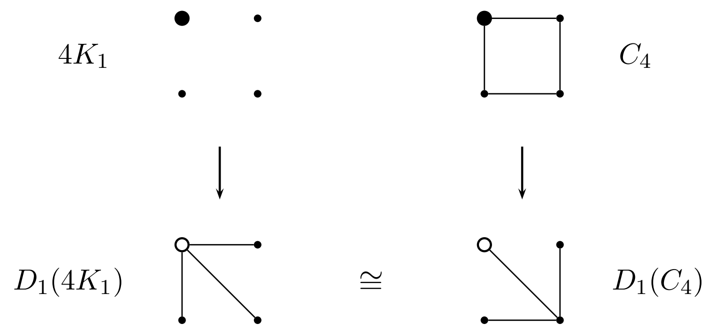

Figure 1: Vertex-reconstruction for $4K_1$ and C_4.

1.2 Reconstruction problems and zeroes of Krawtchouk polynomials

Given a finite, simple graph G with $|V(G)| = n \geq 3$. For $U \subset V(G)$, the switching G_U of G at U is the graph obtained from G by replacing all edges between U and $V(G)\setminus U$ by the nonedges. The multiset of unlabeled graphs $D_s(G) = \{G_U : |U| = s\}$ is called the s-switching deck of G. The *vertex-switching reconstruction problem* asks whether G is uniquely defined up to isomorphism by $D_s(G)$. Stanley [17] pointed out that the vertex-switching reconstruction problem has a negative answer in general, as illustrated by the following simple example: Let G be the totally disconnected graph $4K_1$ on four vertices, respectively, the cycle of length four, C_4. Then, in both cases, $D_1(G)$ consists of the star $K_{1,3}$ only (see Figure 1, where we switched at the left-upper vertex of the graph).

On the other hand, it is natural to ask, which conditions have to be imposed on the underlying graphs in order to solve the reconstruction problem. Many special graphs have been investigated and several bounds on the degree of reconstructible graphs have been shown (cf. [4, 5, 6, 7, 13]). A major result in this area has been obtained by Krasikov and Roditty [13, Remark 2]. They proved an analogue of Kelly's Lemma to reconstruct the number of subgraphs in a graph. To state the result, some more notation is needed. Given graphs G and H, let $X_s(G \to H)$ denote the number of sets $U \subset V(G)$, $|U| = s$, such that G_U is isomorphic to H. Furthermore, let A_s^n denote the matrix with rows and columns indexed by the unlabeled graphs on n vertices, with the (G, H) entry being $X_s(G \to H)$. Denote by

$$P_k^n(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} \tag{1.1}$$

the binary Krawtchouk polynomial of degree k (for more details see Section 2).

Theorem 1.1 (Krasikov/Roditty [13]). *The s-switching deck $D_s(G)$ of G determines the number of induced subgraphs of G isomorphic to a given m-vertex graph provided no eigenvalue of A_1^m is a root y of*

$$R_s^m(y) = \sum_{k=\max(0,s+m-n)}^{\min(m,s)} \binom{n-m}{s-k} P_k^n((m-y)/2).$$

Ellingham [4] used an idea about m-cubes to simplify the result, thus directly relating the reconstruction to the existence of integral roots of Krawtchouk polynomials. Recall that G has n vertices.

Theorem 1.2 (Ellingham [4]). *The s-switching deck $D_s(G)$ of G determines the number of induced subgraphs of G isomorphic to a given m-vertex graph provided $P_s^n(x)$ has no even root in $[0, m]$.*

Several other reconstruction problems relate to integer roots of Krawtchouk polynomials [11]. Mention, for example, the *reorientation reconstruction problem*, which refers to a reconstruction problem for directed graphs. Given a directed graph Γ with $E(\Gamma) = m$. For any $A \subset E$ denote by Γ_A the graph obtained by flipping the orientation of all arcs in A. Similarly as before, define the s-reorientation deck $D_s(\Gamma) = \{\Gamma_A : |A| = s\}$. The reorientation reconstruction problem asks whether Γ is uniquely defined up to isomorphism by $D_s(\Gamma)$. The following connection holds [11]:

Theorem 1.3 (Krasikov/Litsyn [10]). *If $P_s^m(x)$ has no integer root then Γ can be reconstructed.*

A similar connection holds for the *sign reconstruction problem.*

1.3 Outline of chapter

In the present chapter we study integral roots of Krawtchouk polynomials from a Diophantine point of view and prove our main result (see Section 1.4). The chapter is organized as follows: In Section 2 we recall several well-known facts on Krawtchouk polynomials, which we are used in the sequel. Section 3 is devoted to a short account on Diophantine equations of the type $f(x) = g(y)$, where $f, g \in \mathbb{Q}[x]$. Most important, we present the algorithmic criterion for finiteness of solutions of Bilu and Tichy [1]. In Section 4 we recall the discrete Laguerre inequality, a striking result by Krasikov [9]. After presenting the connection of monotonicity of stationary points and indecomposability of polynomials (Section 5), we use Krasikov's result for the stationary points of Krawtchouk polynomials (Section 6) to decompose these polynomials in Section 7. In the final section, Section 8, we treat the remaining possibilities for decomposing the polynomials with the standard pairs. The exposition ends with a short summary and perspectives for future work.

1.4 Main result

Our main result is the following (for the exact notion we refer to Section 3):

Theorem 1.4. *Let $g(x) \in \mathbb{Q}[x]$ with $\deg g \geq 3$ and assume that $n, k \in \mathbb{Z}^+$ with*

$$16 \leq n \leq 100, \qquad \theta(n) \leq k \leq \theta(n) + 10,$$

where

$$\theta(n) = \max\left(7, \left\lceil \frac{17}{40}\, n - \frac{19}{2} \right\rceil\right).$$

Suppose that the Diophantine equation

$$P_k^n(x) = g(y) \tag{1.2}$$

with Krawtchouk polynomials $P_k^n(x)$ has infinitely many rational solutions (x, y) with a bounded denominator. Then we are in one of the following cases.

(i) $g(x) = P_k^n(\tilde{g}(x))$ for some polynomial $\tilde{g} \in \mathbb{Q}[x]$.

(ii) $k = 2k'$, $k' \geq 2$ and $g(x) = \phi(\tilde{g}(x))$, where $\tilde{g}$ is a polynomial over $\mathbb{Q}$, whose square-free part has at most two zeroes, such that $\tilde{g}$ takes infinitely many square values in $\mathbb{Z}$.

2 Krawtchouk polynomials

2.1 Basic facts

The *Krawtchouk polynomials* $P_k^{(p,n)}(x)$ resp. $P_k^n(x)$ often come across while studying combinatorial problems where some sort of involution on the underlying structure takes place. This is well explained by the generating function,

$$\sum_{k=0}^{\infty} P_k^{(p,n)}(x) z^k = \left(1 - \frac{1-p}{p}\, z\right)^x (1+z)^{n-x}. \tag{2.1}$$

According to the Askey-scheme [14] (see also [22, p.35/36]), the (general) Krawtchouk polynomials $P_k^{(p,n)}(x)$ form a family of polynomials which are orthogonal with respect to the discrete measure μ defined by $\mu(i) = \binom{n}{i} p^i (1-p)^{n-i}$, $i = 0, \ldots, n$ with $0 < p < 1$. The special case $p = 1/2$ yields the standard *binary* Krawtchouk polynomials, which – for the sake of shortness – we will denote by $P_k^n(x) = P_k^{(1/2,n)}(x)$. From (1.1) or (2.1) it is easy to derive that

$$P_k^n(x) = \sum_{j=0}^{k} (-2)^j \binom{x}{j} \binom{n-j}{k-j}, \tag{2.2}$$

from which again the uppermost coefficients of

$$P_k^n(x) = c_k x^k + c_{k-1}x^{k-1} + c_{k-2}x^{k-2} + \ldots + c_0$$

follow at once,

$$c_k = \frac{(-2)^k}{k!}, \qquad c_{k-1} = \frac{(-2)^{k-1}n}{(k-1)!}, \qquad c_{k-2} = \frac{(-2)^{k-2}}{6(k-2)!}\,(3n^2 - 3n + 2k - 4), \tag{2.3}$$

$$\begin{aligned} c_{k-3} &= \frac{(-2)^{k-3}n}{6(k-3)!}\,(n^2 - 3n + 2k - 4), \\ c_{k-4} &= \frac{(-2)^{k-2}}{360(k-4)!}\,(20k^2 - 108k - 60kn + 60kn^2 + 150n \\ &\qquad - 90n^3 + 15n^4 - 75n^2 + 112), \\ c_{k-5} &= \frac{(-2)^{k-2}n}{360(k-5)!}\,(20k^2 - 108k - 60kn + 20kn^2 + 150n \\ &\qquad + 5n^2 + 112 + 3n^4 - 30n^3), \text{ etc.} \end{aligned}$$

We also recall the three-term recurrence relation

$$(k+1)P_{k+1}^n(x) = (n-2x)P_k^n(x) - (n-k+1)P_{k-1}^n(x), \qquad k \geq 1, \tag{2.4}$$

and the difference equation

$$(n-x)P_k^n(x+1) = (n-2k)P_k^n(x) - xP_k^n(x-1), \qquad k \geq 0, \tag{2.5}$$

which will be especially important for the method presented in this chapter. Another useful recurrence relation is [10, relation (7)],

$$(n-k+1)P_k^{n+1}(x) = (3n - 2k - 2x + 1)P_k^n(x) - 2(n-x)P_k^{n-1}(x). \tag{2.6}$$

2.2 Zeroes and upper bounds

As for a detailed study of the zeroes of $P_k^n(x)$ (such as interlacing properties, bounds etc.), we refer to [11, 10]. Here we shortly recall some well-known facts, which are crucial for our discussion. One easily notes that

$$P_k^n(n/2) = \begin{cases} (-1)^{k/2}\binom{n/2}{k/2}, & n \text{ even;} \\ 0, & n \text{ odd.} \end{cases} \tag{2.7}$$

The Krawtchouk polynomial $P_k^n(x)$ has k simple roots

$$0 < r_{1,n}(k) < r_{2,n}(k) < \ldots < r_{k,n}(k) < n. \tag{2.8}$$

Since

$$P_k^n(x) = (-1)^k P_k^n(n-x), \tag{2.9}$$

they lie symmetric around the point $x = n/2$. Moreover, for $k < n/2$ the distance between consecutive zeroes decreases towards $n/2$. Also, recall that for $1 \leq k < n/2$ we have

$$r_{i+1,n}(k) - r_{i,n}(k) > 2, \tag{2.10}$$

while for $k < n$ we have $r_{i+1,n}(k) - r_{i,n}(k) > 1$. Levenshtein [15] proved the following explicit formula for the smallest root,

$$r_{1,n}(k) = n/2 - \max\left(\sum_{i=0}^{k-2} x_i x_{i+1} \sqrt{(i+1)(n-i)}\right), \tag{2.11}$$

where the maximum is taken over all $(x_1, \ldots, x_n)$ with $\sum_{i=0}^{k-1} x_i^2 = 1$. It is not difficult to see that

$$r_{1,n}(k) > 1. \tag{2.12}$$

It is well-known that the zeroes of Krawtchouk polynomials for small k can be approximated by the corresponding roots of the Hermite polynomials. If $(n-k) \to \infty$ then the zeroes of $P_k^n(x)$ indeed approach

$$\frac{n}{2} + \frac{\sqrt{n-k-1}}{2}\, h_i(x), \tag{2.13}$$

where $h_1(k) < \ldots < h_k(k)$ are the roots of the Hermite polynomial $H_k(x)$. Finally, mention also a result due to Krasikov [8] which gives a bound of $P_k^n(x)$ at integer values provided $k \leq n/2$. Let $q = 2\sqrt{k(n-k)}$, then it holds

$$(P_k^n(x))^2 \leq \frac{x!(n-x)!}{\lfloor \frac{k}{2} \rfloor !^2 \lfloor \frac{n-k}{2} \rfloor !^2}\, \tau(n,k,x), \qquad x = 0, 1, \ldots, \lfloor n/2 \rfloor, \tag{2.14}$$

where $\tau(n,k,x)$ is

$$\frac{q^2+2n}{4(n-x)}, \quad n, k \text{ even}; \qquad \frac{4}{n-x}, \quad n \text{ even}, k \text{ odd};$$
$$\frac{2k+1}{n-x}, \quad n \text{ odd}, k \text{ even}; \qquad \frac{2n-2k+1}{n-x}, \quad n, k \text{ odd}.$$

In the vicinity of $n/2$ there are better estimates available [8].

3 The Diophantine equation $P_k^n(x) = g(y)$

3.1 Introduction

The integrality of zeroes of Krawtchouk polynomials relates to the study of the solution set of the one-variable Diophantine equation

$$P_k^n(x) = 0 \tag{3.1}$$

in rational integers x. Much interest has been focused on classifying the zeroes for certain values of k and n (see [11]). For instance, the zeroes are completely classified for $k \leq 7$, for $k = (n-t)/2$ with $t \leq 6$ and $t = 8$ when the root is odd. It is conjectured, that for any choice of the pair (k, n) the number of integral zeroes does not exceed 4. On the other hand, there are also results of a typical Diophantine nature. For example, for every $k \geq 4$, the polynomial $P_k^n(x)$ can have nontrivial integer roots only for finitely many values n.

An interesting generalization is to allow an arbitrary rational polynomial $g(y)$ on the right hand side of (3.1),

$$P_k^n(x) = g(y), \tag{3.2}$$

which makes up the hub of the present chapter. How many integral solutions (x, y) does (3.2) have? Is it possible to find an infinite set of solutions which can be constructed via a suitable integer-valued parametrization?

The study of Diophantine equations of the shape $f(x) = g(y)$ has a long history. In order to settle the problem of finiteness of integral solutions (x, y) for a specific equation (i.e. without parameters involved), one can resort to Siegel's theorem on integral points on algebraic curves [16]. The procedure is as follows: First, one computes the genus of the algebraic curve under question, and in case of zero genus one calculates the number of points at infinity to conclude. If the polynomials f and g itself depend on several parameters (e.g., on k and n in (3.2)), such a direct calculation is not possible. In 2000, Bilu and Tichy [1], while extending work of Davenport, Ehrenfeucht, Fried, Lewis, MacRae, Ritt, Schinzel, Siegel and others, proved an algorithmic criterion which makes it possible to apply Siegel's theorem also in the multi-parametric case.

3.2 The criterion of Bilu and Tichy

In order to formulate the criterion we need the definition of the five so-called *standard pairs* (over $\mathbb{Q}$). In what follows, let $\gamma, \delta \in \mathbb{Q} \setminus \{0\}$, $q, s, t \in \mathbb{Z}_{>0}$, $r \in \mathbb{Z}_{\geq 0}$ and $v(x) \in \mathbb{Q}[x]$ a non-zero polynomial (which may be constant). We also make use of the *Dickson polynomials* which can be defined by

$$D_s(x, \gamma) = \sum_{i=0}^{\lfloor s/2 \rfloor} d_{s,i} x^{s-2i} \quad \text{with} \quad d_{s,i} = \frac{s}{s-i} \binom{s-i}{i} (-\gamma)^i. \tag{3.3}$$

We say that the equation $f(x) = g(y)$ has *infinitely many rational solutions with a bounded denominator*, if there is $\nu \in \mathbb{Z}^+$ such that $f(x) = g(y)$ has infinitely many rational solutions (x, y) with $\nu x, \nu y \in \mathbb{Z}$. If an equation has only finitely many rational solutions with a bounded denominator then, in particular, it has only finitely many solutions in integers.

The list of *standard pairs* (over $\mathbb{Q}$), which is referred to in Theorem 3.1, includes five different pairs of polynomials (f_1, g_1).

A standard pair of the *first* kind is of the type

$$(x^q, \gamma x^r v(x)^q) \tag{3.4}$$

(or switched), where $0 \le r < q$, $\gcd(r, q) = 1$ and $r + \deg v > 0$.

A standard pair of the *second* kind is given by

$$(x^2, (\gamma x^2 + \delta) v(x)^2) \tag{3.5}$$

(or switched).

A standard pair of the *third* kind is

$$(D_s(x, \gamma^t), D_t(x, \gamma^s)) \tag{3.6}$$

with $s, t \ge 1$ and $\gcd(s, t) = 1$.

A standard pair of the *fourth* kind is

$$(\gamma^{-s/2} D_s(x, \gamma), -\delta^{-t/2} D_t(x, \delta)) \tag{3.7}$$

(or switched) with $s, t \ge 1$ and $\gcd(s, t) = 2$.

A standard pair of the *fifth* kind is of the form

$$((\gamma x^2 - 1)^3, 3x^4 - 4x^3) \tag{3.8}$$

(or switched).

We are now ready to state the criterion of Bilu and Tichy [1].

Theorem 3.1 (Bilu/Tichy [1])**.** *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent:*

(i) The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.

(ii) We can express $f \circ \kappa_1 = \phi \circ f_1$ and $g \circ \kappa_2 = \phi \circ g_1$ where $\kappa_1, \kappa_2 \in \mathbb{Q}[x]$ are linear, $\phi(x) \in \mathbb{Q}[x]$, and (f_1, g_1) is a standard pair over $\mathbb{Q}$.

Observe that if we were able to get a contradiction for decompositions of f and g as demanded in (i) of Theorem 3.1, then finiteness of the number of integral solutions (x, y) of the original Diophantine equation $f(x) = g(y)$ is guaranteed. Tichy and the author [21] used the special form of the leading coefficient c_k in (2.3) to prove

Theorem 3.2 (Stoll/Tichy [21])**.** *Let n and m be distinct integers satisfying $m, n \ge 3$. Further let $N \ge \max(m, n)$ and $p_1, p_2 \in \mathbb{Q} \setminus \{0, 1\}$. Then the equation*

$$\binom{N}{m} P_n^{(p_1,N)}(x) = \binom{N}{n} P_m^{(p_2,N)}(y) \tag{3.9}$$

has only finitely many solutions in integers (x, y).

Despite the generality of Theorem 3.2, which addresses general Krawtchouk polynomials $P_k^{(p,n)}(x)$ (recall (2.1)), it is not possible to extend the proof to remove the binomial coefficient factors in (3.9). The aim of the present chapter is to outline a method, which uses a ingenious tool from the geometry of polynomials to get a finiteness result of the same shape for (3.2).

4 The discrete Laguerre inequality

4.1 Introduction and statement

In order to apply Theorem 3.1 in the most general form for the binary Krawtchouk polynomials one has to prove a general decomposition theorem for $P_k^n(x)$ and to exclude possible decompositions involving the standard pairs. While this is rather straightforward for the classical continuous orthogonal polynomials (Laguerre, Hermite, Jacobi) [20], it has not even been proved for a single family of discrete classical orthogonal polynomials (Krawtchouk, Meixner, Meixner-Pollaczek, Hahn, Wilson, Charlier etc.). At least, due to the similarity to Hermite polynomials (2.13), one may strongly expect an analogous result for Krawtchouk polynomials. We here use a method due to Krasikov [9] to get a first result in this direction. We do not aim to optimize our argument; indeed, in the end, we will use concrete numerical data in place of the general parameters k and n. However, with more technical efforts it is possible to enlarge the parameter sets in our main theorem and to get a statement for polynomials $P_k^n(x)$ with $k = k(n)$ as well.

The classical Laguerre inequality states that for any polynomial $f \in \mathbb{R}[x]$ with only real zeroes there holds $f'^2 - ff'' \geq 0$. A higher degree generalization has been obtained by Jensen and used by Patrick (see [9] for the references), namely,

$$L_m(f) = \sum_{j=-m}^{m} (-1)^{m+j} \, \frac{f^{(m-j)}(x) f^{(m+j)}(x)}{(m-j)!(m+j)!} \geq 0. \tag{4.1}$$

In 2003, Krasikov [9] showed a surprising difference analogue of (4.1). Let $x_1 < x_2 < \cdots < x_n$ be the zeroes of $f(x)$ and denote by $M(f)$ the mesh defined by $M(f) = \min_{2 \leq i \leq n}(x_i - x_{i-1})$.

Theorem 4.1 (Krasikov [9])**.** *Let* $M(f) \geq \sqrt{4 - \frac{6}{m+2}}$, *then*

$$V_m(f) = \sum_{j=-m}^{m} (-1)^j \, \frac{f(x-j)f(x+j)}{(m-j)!(m+j)!} \geq 0. \tag{4.2}$$

Relation (4.2) can be used to get explicit inequalities on the size of polynomials, respectively, to bound the extreme zeroes.

4.2 Krasikov's application to Krawtchouk polynomials

A nice application to Krawtchouk polynomials has been outlined in [9]. Therein, Theorem 4.1 is used with $m = 2$ to get very sharp envelopes for $P_k^n(x)$ with $k < n/2$. As we will need these numerical data in our investigations, we recall the method and the calculations from [9] (we also fix a misprint in (4.4)).

By the difference relation (2.5) it is possible to write $V_2(P_k^n)$ only in terms of $P_k^n(x)$ and $P_k^n(x-1)$. Moreover, by (2.10) the mesh condition of Theorem 4.1 is satisfied. This gives

$$V_2(P_k^n) = \frac{A(x)t^2 + B(x)t + C(x)}{12(n-x)(n-x-1)(x-1)}\,(P_k^n(x))^2 \geq 0, \tag{4.3}$$

where $t = t(x) = P_k^n(x-1)/P_k^n(x)$ and

$$\begin{aligned}
A(x) &= -x(4x^2 - 4nx + 4n + m^2 - 4),\\
B(x) &= m(4x^2 - 4nx + 2x + 3n + m^2 - 4),\\
C(x) &= 4x^3 - 8nx^2 + (4n^2 + 2n + m^2 - 4)x - 2n^2 - m^2 n + 4n - m^2,
\end{aligned}$$

with $m = n - 2k$. Note that by (2.8) and (2.12) the denominator in (4.3) is positive. Having at hands (4.3), it is possible to derive bounds on $P_k^n(x)$ and $P_k^n(x-1)$ inside the oscillatory region. This is obtained by looking at the ellipse described by V_2. Define

$$\begin{aligned}
W(x) &= \frac{V_2(P_k^n(x+1)) - zV_2(P_k^n(x))}{(P_k^n(x))^2}\\
&= \frac{x\alpha(x)t^2 - m\beta(x)t - (n-x-2)\gamma(x)}{12(n-x)^2(n-x-2)(n-x-1)(x-1)},
\end{aligned} \tag{4.4}$$

where

$$\begin{aligned}
\alpha(x) = {}&(n-x-2)(n-x)(4x^2 - 4xn + m^2 + 4n - 4)z\\
&+ (x-1)(4x^3 + (12-8n)x^2 + (4n^2 - 14n + m^2 + 8)x\\
&\quad - n(m^2 - 2n + 2)),\\
\beta(x) = {}&(n-x-2)(n-x)(m^2 + 3n - 4xn + 2x + 4x^2 - 4)z\\
&+ (x-1)(4x^3 + (14-8n)x^2 + (m^2 - 17n + 4n^2 + 14)x\\
&\quad - n(m^2 + 2 - 3n)),\\
\gamma(x) = {}&(n-x)(4x^3 - 8x^2 n + (m^2 + 4n^2 + 2n - 4)x + 4n\\
&- nm^2 - m^2 - 2n^2)z - (x-1)(4x^3 + (4-8n)x^2\\
&\quad + (m^2 - 8n + 4n^2)x + n^2 - 12k^2 - nm^2 + 12nk).
\end{aligned}$$

Note that the discriminant $m^2\beta(x)^2 + 4x(n-x-2)\alpha(x)\gamma(x)$ can be interpreted as a quadratic polynomial in z. We choose z from setting the discriminant equal to zero, in which case the signs of $W(x)$ and $\alpha(x)$ coincide. This yields,

$$z_{1,2}(x) = \frac{(x-1)(\triangle(x+\frac{1}{2}) - 3S \pm 6\sqrt{R})}{(n-x-2)\triangle(x)},$$

where (with the abbreviation $y = n - 2x$),

$$\begin{aligned}
\triangle(x) &= (y^2 - (n-1)^2 + m^2 - 1)^3 - 2(y^2 + m^2 - 1)^2 + m^2y^2 \\
&\quad + 2(n-1)^2(n^2 - 2n + 5), \\
S &= y(y-2)(y-1)^2 - (n^2 - 2n - m^2 + 2)^2 + 7(n-1)^2, \\
R &= (n^2 - y^2 - 2n + 2y)(n^2 - m^2)((n-2)^2 - m^2)((n-1)^2 \\
&\quad - m^2 - (y-1)^2).
\end{aligned}$$

Recall, that $\triangle(x) < 0$ in the oscillatory region [8], provided that

$$2 \leq k < \frac{n}{2} - 2 \cdot 3^{-3/4}\sqrt{n}. \tag{4.5}$$

Within this range we therefore have

$$z_1(x) \leq \frac{V_2(P_k^n(x+1))}{V_2(P_k^n(x))} \leq z_2(x). \tag{4.6}$$

As Krasikov points out, one can use $V_2(P_k^n(n/2))$ as an initial value in (4.6) to obtain upper bounds for $P_k^n(n/2+i)$, $i \geq 1$, consecutively. For our purpose, we need explicit *upper and lower bounds for the maximum of* $P_k^n(x)$ between consecutive zeroes, i.e. for *real* x in the interval $[x_{i-1}, x_i]$. This is motivated by the connection of monotonicity of stationary points to decomposability of polynomials, which is the subject of the next section.

5 Monotonicity of stationary points and indecomposability

5.1 Definitions

Polynomial decomposition theory is aimed at a characterization of all representations of a given polynomial $f = \phi \circ h \in \mathbb{R}[x]$, where $\phi, h \in \mathbb{R}[x]$, $\min(\deg \phi, \deg h) \geq 2$ and "$\circ$" denotes the functional composition applied for polynomials[1]. The left term ϕ is called the *left* and the right term h the *right component* of the decomposition. Two decompositions $f = \phi_1 \circ h_1 = \phi_2 \circ h_2$ are called *equivalent* (and thus regarded as basically the same), if there is a linear polynomial κ such that $\phi_2 = \phi_1 \circ \kappa$ and $h_2 = \kappa^{-1} \circ h_1$. A polynomial f is called *decomposable* (over $\mathbb{R}$) if it has at least one non-trivial decomposition with real components.

[1] More precisely, such a decomposition is called a *non-trivial decomposition.*

5.2 Decomposition and orthogonal polynomials

Orthogonal polynomials – besides having simple real zeroes – have simple stationary points. A main theme, for instance in approximation theory, is to prove a monotonicity result for the extremal points of the polynomials under question. Denote by

$$\delta(f;\gamma) = \deg\gcd(f-\gamma, f'), \quad \gamma \in \mathbb{R},$$

which counts the number of stationary points of $f(x)$ with equal ordinate value. An important connection to polynomial decomposition theory is given by the following fact [3].

Lemma 5.1 (Dujella/Tichy [3]). *Let $f = \phi \circ h$, where $\phi, h \in \mathbb{R}[x]$. If $\deg\phi \geq 2$, then there exists $\gamma \in \mathbb{R}$ with $\delta(f;\gamma) \geq \deg h$. In particular, if $\delta(f;\gamma) \leq s$ for all $\gamma \in \mathbb{R}$ then $\deg h \leq s$.*

According to Lemma 5.1 we have $\deg h \leq s \in \mathbb{Z}_{>0}$ provided that there are at most s intervals for which the stationary points of $f(x)$ are monotone increasing/decreasing on the respective intervals. In that context we recall a result due to Tichy and the author [20].

Theorem 5.2 (Stoll/Tichy [20]). *Let $f(x) \in \mathbb{R}[x]$ with only real zeroes satisfy*

$$\sigma(x)f''(x) + \tau(x)f'(x) - \lambda(x)f(x) = 0, \tag{5.1}$$

with $\sigma(x) = ax^2 + bx + c$, $\tau(x) = dx + e$ and $a, b, c, d, e \in \mathbb{R}$, $ad \neq 0$. Furthermore, suppose that $\sigma'(x) - 2\tau(x)$ does not vanish identically. Then $\delta(f;\gamma) \leq 2$ for all $\gamma \in \mathbb{R}$.

The general continuous classical orthogonal polynomials (Laguerre, Jacobi, Hermite) satisfy (5.1), whereas the Chebyshev polynomials exactly make up the exceptional case of Theorem 5.2.[2] However, for Krawtchouk polynomials there is no differential equation of Sturm-Liouville type available, such that one has to use another method.

6 Stationary points of Krawtchouk polynomials

6.1 Iteration of Krasikov's bound

The present section is devoted to a detailed study of relation (4.6) which delivers the needed information to bound $\delta(P_k^n;\gamma)$ for all $\gamma \in \mathbb{R}$. To start

[2] In fact, it is well-known that the standard (*non-monic*) Chebyshev polynomials of the first kind $T_k(x)$ have all stationary points of equal ordinate value. Moreover, they are decomposable for any non-prime k by the relation $T_m(T_n(x)) = T_n(T_m(x)) = T_{mn}(x)$.

with, iterating (4.6) yields

$$\rho_1(x) := V_2\left(P_k^n\left(\{x-\frac{n}{2}\}+\frac{n}{2}\right)\right)\prod_{i=0}^{\lfloor x\rfloor-\frac{n}{2}-1} z_1\left(\{x-\frac{n}{2}\}+\frac{n}{2}+i\right) \tag{6.1}$$
$$\leq V_2(P_k^n(x))$$
$$\leq V_2\left(P_k^n\left(\{x-\frac{n}{2}\}+\frac{n}{2}\right)\right)\prod_{i=0}^{\lfloor x\rfloor-\frac{n}{2}-1} z_2\left(\{x-\frac{n}{2}\}+\frac{n}{2}+i\right) =: \rho_2(x).$$

Herein, $\{x\} = x - \lfloor x\rfloor$ denotes the fractional part of x. It may be possible to relax (6.1) in order to improve on our results, but only at the cost of extensive computational work. In fact, while z_1, z_2 are monotone increasing functions in the oscillatory region, this behaviour changes near the extreme zeroes and one has to use more tricky arguments (see [7]). Moreover, it is a rather (computationally) complex task to prove that $V_2(P_k^n(x))$ takes its minimal resp. maximal value on $[n/2, n/2+1]$ at the left resp. right point of the interval (one may use (2.6), (2.7) and (4.3)).

Now, consider (4.3) and the ellipse with

$$A(x)t^2 + B(x)t + C(x) = \text{const.} \tag{6.2}$$

The upper bound for $\max_{x_i<x<x_{i+1}} P_k^n(x)$ follows by calculating the major axis of (6.2). This gives (we omit the details)

$$\lambda(x) = \frac{A(x)+C(x)}{2} - \frac{1}{2}\sqrt{A(x)^2 - 2A(x)C(x) + C(x)^2 + B(x)^2}$$

and

$$P_k^n(x) \leq \sqrt{\frac{\rho_2(x)}{\lambda(x)}} =: u(x), \qquad n/2 \leq x \leq x_n. \tag{6.3}$$

On the other hand, considering the minor axis yields that for all $i = 1, \ldots, n$ there exists $x \in [x_{i-1}, x_i]$ such that

$$P_k^n(x) \geq \sqrt{\frac{\rho_1(x)}{C(x)}} := l(x). \tag{6.4}$$

We illustrate these two bounds in Figure 2 for the case $n = 100$, $k = 21$.

Obviously, comparing the upper and lower bound it is possible to get a bound for the number of stationary points of equal ordinate value.

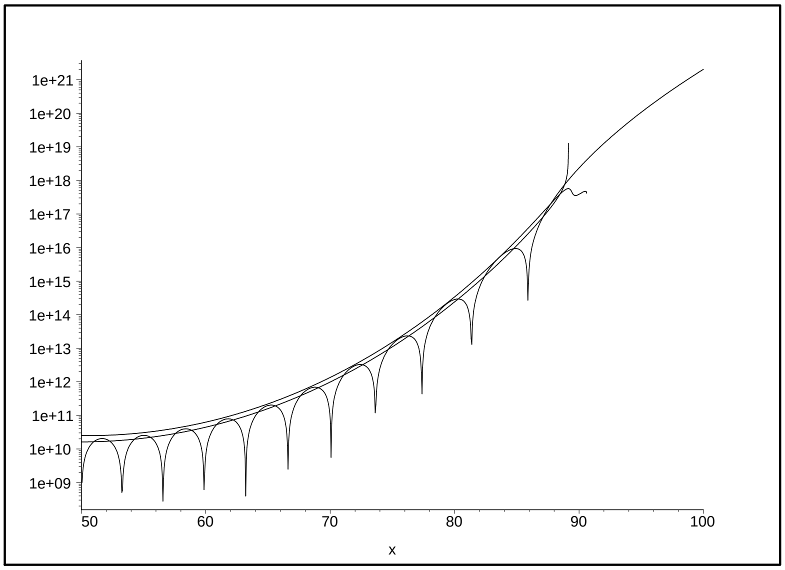

Figure 2: $|P_{21}^{100}(x)|$ on a logarithmic scale

6.2 Admissible parameter ranges

We use a very rough criterion to conclude, namely (motivated by (2.10)), if

$$\min\{1 \leq j \leq n/2 : \quad l(n/2 + 2j) > u(n/2 + j)\} = s \tag{6.5}$$

then $\delta(P_k^n; \gamma) \leq 2s$. For every $n \leq 100$ we have calculated the values for k subject to (4.5) which satisfy (6.5) with $s \leq 3$. The data is illustrated in Figure 3.[3] From the plot we see that the bounds are most helpful in the vicinity of the bound in (4.5), which is the upper envelope of the represented points.

According to Lemma 5.1, for the values (n, k) given in Figure 3 (which we will call *admissible* in the sequel) we have that $P_n^k(x) = \phi(h(x))$ with $\phi, h \in \mathbb{R}[x]$ implies $\deg h \leq 6$. In the next section we will deal with these possible decompositions by a recent method proposed by the author [19]. Observe that the set referred to in Theorem 1.4, i.e.,

$$16 \leq n \leq 100, \qquad \theta(n) \leq k \leq \theta(n) + 10,$$

with

$$\theta(n) = \max\left(7, \left\lceil \frac{17}{40}\, n - \frac{19}{2} \right\rceil\right),$$

is a subset of the *admissible pairs* (n, k).

[3] One may considerably improve these estimates for k odd, however, we will aim for a more uniform result.

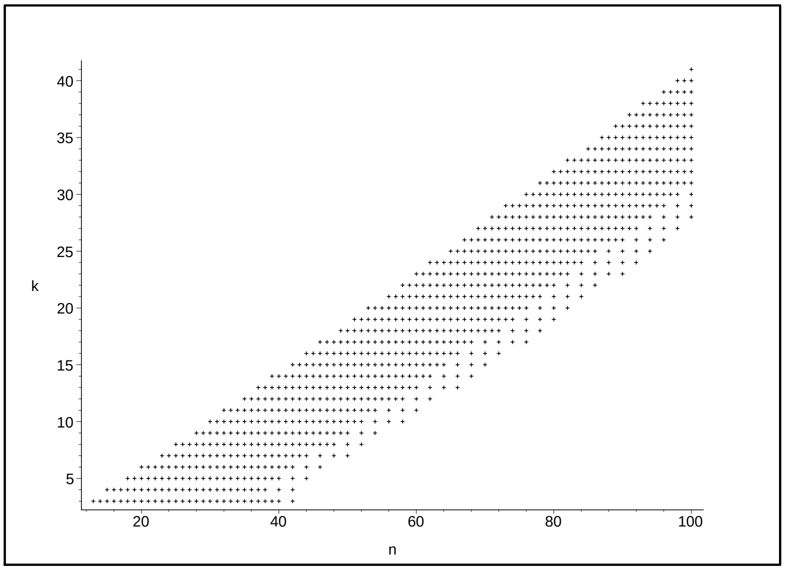

Figure 3: Values of (n,k) with $P_n^k(x)$ having at most 6 stationary points of equal value

7 Decomposition of Krawtchouk polynomials

7.1 An indecomposability criterion

Given a polynomial $f(x) \in \mathbb{R}[x]$ and suppose that there is a decomposition of the form

$$f = \phi \circ h \tag{7.1}$$

with $\deg h = s$ being a small number (in our case ≤ 6). One way to disprove that there cannot exists such a decomposition consists in comparing coefficients on both sides of the decomposition equation (7.1). Since the uppermost coefficients of f (cf. (2.3)) are given, one may try to come to a contradiction while equating with the parametric coefficients on the right hand side of (7.1). An algorithmic, well-organized way of performing this task has recently been given by the author [18, 19]. We recall the main ingredients. First, a polynomial $\hat{h}$ of degree s is computed which is the *only* (normed) candidate of degree s which could make up a right decomposition factor for f (see [19, Algorithm 1]). Using $\hat{h}$ we have at hands a convenient algorithmic criterion for impossibility of polynomial decomposition.

Lemma 7.1 (Stoll [18]). *Let f be monic and $s \geq 2$ a positive integer. Furthermore, let*

$$f(x) = \hat{h}(x)^k + \beta_1 \hat{h}(x)^{k-1} + \cdots + \beta_l \hat{h}(x)^{k-l} + \mathcal{R}(x), \tag{7.2}$$

for some constants $\beta_j \in \mathbb{R}$, $0 \leq l \leq k$ with $\deg \mathcal{R} \leq sk - s$ and $m \nmid \deg R$. Then f is indecomposable with right components of degree s.

From a practical point of view, Lemma 7.1 fits best the problem, when the degree of $\hat{h}$ is small. In fact, given $f(x)$, one expands $f(x)$ regarding $\hat{h}(x)$ up to sufficiently large order (indicated by l) such that the remainder polynomial $\mathcal{R}(x)$ has the wanted properties. Regarding the Krawtchouk polynomials with parameter constrictions given in Figure 3, we have to come to a contradiction when considering right decomposition factors with $\deg h \leq 6$. In the sequel, we give an outline of these calculations. For more details on the computational aspects (addressing both the Gröbner bases and the implementation issues) we refer the interested reader to the article [19].

7.2 Application to Krawtchouk polynomials

The main result which will be proved in the remaining part of this section is the following:

Theorem 7.2. *Suppose* $P_k^n(x) = \phi(h(x))$ *with* $\phi(x), h(x) \in \mathbb{R}[x]$ *and* $2 \leq \deg h \leq 6$. *Then* $\deg h = 2$ *and the decomposition is equivalent to*

$$P_k^n(x) = \hat{\phi}(x^2 - nx) \tag{7.3}$$

for some unique polynomial $\hat{\phi}(x) \in \mathbb{Q}[x]$.

To start with the proof, let $\deg h = 2$. By (2.9) we see that $P_{2k}^n(x) = P_{2k}^n(n-x)$ from which easily follows that there are unique polynomials $\phi_1(x), \phi_2(x) \in \mathbb{Q}[x]$ with

$$P_{2k}^n(x) = \phi_1\left((x - n/2)^2\right) = \phi_2\left(x^2 - nx\right),$$

which is (7.3).

The only possible candidate of degree 3 (we use the first algorithm given in [19]) is

$$\hat{h}(x) = x^3 - \frac{3}{2}nx^2 + \left(\frac{9}{4}k^2 - \frac{9}{8}kn - \frac{9}{4}k + \frac{3}{4}n^2 + \frac{3}{8}n + \frac{1}{2}\right)x.$$

Taylor expansion with respect to this polynomial (use the second algorithm of [19]) leads to

$$\begin{aligned} P_{3k}^n(x) = \hat{h}(x)^k &- \frac{1}{16}nk(18k^2 - 18k - 9nk + 4 + 2n^2 + 3n)\,\hat{h}(x)^{k-1} \\ &- \frac{9}{540}k(3k-1)(k-1)(48k^2 - 56k - 30kn + 16 + 20n + 5n^2)\,x^{3k-4} \\ &+ O(x^{3k-5}). \end{aligned}$$

Lemma 7.1 implies that in the equation above we have $[x^{3k-4}] = 0$, giving

$$n = k - \frac{1}{2} + \frac{1}{6}\sqrt{-60k^2 + 108k - 39}.$$

The expression under the square root symbol is ≥ 0 if and only if

$$\frac{1}{2} \leq k \leq \frac{13}{10} < 2,$$

a contradiction. Thus, there cannot exist a decomposition of a Krawtchouk polynomial $P_k^n(x)$ with right component of degree three.

The calculations for $\deg h = 4$ are much more involved. First suppose that $k \geq 3$. We start with the expansion

$$\begin{aligned} P_{4k}^n(x) = \hat{h}(x)^k + &\beta_1 \hat{h}(x)^{k-1} + r_1 x^{4k-6} + r_2 x^{4k-7} \\ &+\beta_2 \hat{h}(x)^{k-2} + r_3 x^{4k-9} + r_4 x^{4k-10} + O(x^{4k-11}), \end{aligned}$$

which yields $r_1 = r_2 = r_3 = r_4 = 0$. The equations for r_1, r_2, r_3 are basically the same (see below), so that we need one further (independent) equation to conclude. The four equations are

$$\begin{aligned} &k(k-1)(2k-1)(4k-1)(-63488k^3 + 102592k^2 + 46368k^2n - 52528k \\ &\quad - 51408kn - 11340kn^2 + 8192 + 13734n + 6615n^2 + 945n^3) = 0, \end{aligned}$$

$$\begin{aligned} &nk(k-1)(4k-1)(2k-1)(2k-3)(-63488k^3 + 102592k^2 + 46368k^2n - 52528k \\ &\quad - 51408kn - 11340kn^2 + 8192 + 13734n + 6615n^2 + 945n^3) = 0, \end{aligned}$$

$$\begin{aligned} &n^3k(k-1)(k-2)(4k-1)(2k-1)(2k-3)(4k-7)(-63488k^3 + 102592k^2 \\ &\quad + 46368k^2n - 52528k - 51408kn - 11340kn^2 + 8192 + 13734n \\ &\quad + 6615n^2 + 945n^3) = 0, \end{aligned}$$

$$\begin{aligned} &k(k-1)(k-2)(4k-1)(2k-1)(2k-3)(-380764160 + 3731295872k - 855679440n \\ &\quad - 763247100n^2 - 436104900n^3 + 226600605n^4 + 656537805n^5 \\ &\quad + 337265775n^6 + 49116375n^7 + 4552320960kn^2 - 1791912540kn^4 \\ &\quad - 8016988320k^2n^3 + 6200551104kn - 3051556200kn^5 + 2789111160kn^3 \\ &\quad - 908730900kn^6 - 49896000kn^7 - 10817991360k^2n^2 + 671101200k^2n^6 \\ &\quad + 12474000k^2n^7 - 16177793280k^2n - 9804833280k^4n^3 + 4726600560k^2n^4 \\ &\quad + 612057600k^4n^5 + 12445614720k^3n^3 - 149688000k^3n^6 - 12401326080k^4n^2 \\ &\quad - 5779583040k^3n^4 + 4749267600k^2n^5 + 16998812160k^3n + 14100514560k^3n^2 \\ &\quad - 2907273600k^3n^5 - 2681733120k^6n^2 + 2964234240k^5n^3 - 838041600k^5n^4 \\ &\quad - 9931874304k^5n - 1421629440k^4n + 3492910080k^4n^4 + 7937740800k^5n^2 \\ &\quad + 8102150144k^6 - 3575644160k^7 + 24003993600k^3 - 18583019520k^4 \\ &\quad + 402751488k^5 - 13733508864k^2 + 5293178880k^6n) = 0. \end{aligned}$$

With the aid of the Gröbner-package in MAPLE we get the *complete* solution set

$$\{\{k=-1/4,n=-2\},\{k=1/4,n=-3\},\{k=-1,n=-5\},\{k=1/4,n=-6\}$$
$$\{k=-1/2,n=-3\},\{k=1/4,n=n\},\{k=5/4,n=2\},\{k=1/2,n=-4\},$$
$$\{k=1/2,n=n\},\{k=0,n=n,\},\{k=1/4,n=2/3\},\{k=1,n=n\},$$
$$\{k=1/2,n=2/3\},\{k=1,n=2/3\},\{k=1/2,n=-8\},\{k=1,n=-6\},$$
$$\{k=1/4,n=-8\},\{k=1/2,n=-2\},\{k=1/2,n=2\},\{k=-1/2,n=-6\},$$
$$\{k=1/2,n=-3\},\{k=1/2,n=-6\},\{k=3/4,n=2/3\},\{k=-1,n=-8\},$$
$$\{k=-1,n=-6\},\{k=13/36,n=-50/27\},\{k=1/2,n=-5\},\{k=-1/2,n=-4\},$$
$$\{k=105057/2998036Z_2^2+1848969/2998036Z_2+1696531/2998036,n=2\},$$
$$\{k=3/2,n=Z_3/3\},\{k=2,n=Z_1\},\}.$$

Herein, Z_1,Z_2,Z_3, respectively, satisfy the equations

$$\begin{aligned}7Z_1^3-119Z_1^2+714Z_1-1440&=0,\\ 105057Z_2^3+316794Z_2^2-759285Z_2+193378&=0,\\ Z_3^3-33Z_3^2+390Z_3-1544&=0.\end{aligned}$$

No member in the solution set satisfies the integrality constraints for k and n. One easily comes to a contradiction also for $k=2$ by inspecting the single equation $r_1=0$.

Next, assume $\deg h=5$. We here get the expansion

$$P_{5k}^n(x)=\hat{h}(x)^k+\beta_1\hat{h}(x)^{k-1}+r_1x^{5k-6}+r_2x^{5k-7}+r_3x^{5k-8}+O(x^{5k-9}),$$

where

$$\begin{aligned}\beta_1=-\frac{1}{2304}nk(&-5000k^4-3750nk^3+15000k^3+4125n^2k^2-1500nk^2\\ &-11000k^2-900n^3k-1800n^2k+1950nk+3000k\\ &+180n^3+195n^2-300n-272+72n^4)=0.\end{aligned}$$

Obviously $r_1=0$. The equation $r_2=0$ does not yield any new information on the parameters k and n with respect to the first equation. We therefore need also $r_3=0$. More explicitly,

$$\begin{aligned}&nk(k-1)(5k-1)(5k-6)(-740000k^4+409500k^3n+1254000k^3\\ &\quad-535500k^2n-75600k^2n^2-774800k^2+229320kn+68040kn^2\\ &\quad+4725kn^3+205440k-19520-32256n-15120n^2-2079n^3)=0,\end{aligned}$$

$$
\begin{aligned}
&k(5k-1)(k-1)(11101440 - 164212480k + 22925952n + 6119568n^2 \\
&\quad - 11716488n^3 - 7169715n^4 - 1047816n^5 + 377751000k^3n^2 - 452655000k^4n^3 \\
&\quad - 2641350000k^5n - 3186633600k^3 - 22680000k^4n^4 - 850672500k^4n^2 \\
&\quad + 4046100000k^4n - 3086382000k^3n + 77962500k^3n^4 + 604894500k^3n^3 \\
&\quad + 1417500k^3n^5 - 373577400k^2n^3 + 1266640800k^2n + 5907912000k^4 \\
&\quad - 267948480kn - 4309200k^2n^5 - 22427700k^2n^2 - 91868175k^2n^4 \\
&\quad - 6278640000k^5 - 29378400kn^2 + 4003020kn^5 + 107764020kn^3 \\
&\quad + 43630650kn^4 + 3478800000k^6 - 740000000k^7 + 631500000k^6n \\
&\quad - 222000000k^6n^2 + 754950000k^5n^2 + 122850000k^5n^3 + 990888000k^2) = 0.
\end{aligned}
$$

This system of equations has no admissible solution.[4]

Finally, consider $\deg h = 6$. We use the three coefficient equations $[x^{6k-7}] = [x^{6k-8}] = [x^{6k-9}] = 0$ to conclude that there is no admissible solution pair (n, k). For the sake of completeness, we append the three relevant equations,

$$
\begin{aligned}
&k(k-1)(6k-1)(3k-1)(2k-1)(2598912k^4 - 4133376k^3 - 1626480k^3n \\
&\quad + 2393664k^2 + 381780k^2n^2 + 1980000k^2n - 39900kn^3 - 317520kn^2 \\
&\quad - 585696k - 781860kn + 49152 + 1575n^4 + 97960n + 64575n^2 + 17150n^3) = 0,
\end{aligned}
$$

$$
\begin{aligned}
&n(107773725352722432k - 67223682337996800 - 75805048910774400k^2 \\
&\quad - 8055435775759680k^4 + 30850177972149600k^3 + 1034250n^3k^2 \\
&\quad + 80325n^4k^2 - 175659840nk^9 - 1495000800nk^7 - 6300n^4k + 799372800nk^8 \\
&\quad - 4309200n^3k^7 + 41232240n^2k^8 + 1505800800nk^6 - 171732960n^2k^7 \\
&\quad + 285064920n^2k^6 + 170100n^4k^6 - 567000n^4k^5 - 244981800n^2k^5 \\
&\quad + 16216200n^3k^6 + 1411897888929696k^5 + 13511581833600k^7 \\
&\quad - 696037950720k^8 + 19669174272k^9 - 168416458660800k^6 - 23291100n^3k^5 \\
&\quad - 897154020nk^5 + 324647400nk^4 + 16294950n^3k^4 + 118297935n^2k^4 \\
&\quad + 675675n^4k^4 - 5876500n^3k^3 - 32185440n^2k^3 - 352800n^4k^3 \\
&\quad - 69737900k^3n + 8123400k^2n + 4563405k^2n^2 - 258300kn^2 - 68600kn^3 \\
&\quad - 391840kn) = 0,
\end{aligned}
$$

[4] Again, we used MAPLE-V11 to perform the computations.

$$
\begin{aligned}
&k(k-1)(6k-1)(3k-1)(2k-1)(-19660800+314930688k-45724800n\\
&\quad -19203888n^2+23587740n^3+22753500n^4+6592740n^5+623700n^6\\
&\quad -1651985280k^5n^2+1648896480k^4n^2+1197302040k^4n^3-10152980640k^4n\\
&\quad +75592440k^4n^4-537604848k^3n^2+7281972720k^3n-7900200k^3n^5\\
&\quad -267899940k^3n^4-1584615780k^3n^3+311850k^2n^6+945784290k^2n^3\\
&\quad +113532012kn^2+568854176kn-147192045kn^4-2831232624k^2n\\
&\quad +318468150k^2n^4-119138184k^2n^2+25467750k^2n^5-883575kn^6\\
&\quad -24759735kn^5-253449185kn^3-1802756736k^6n-322043040k^5n^3\\
&\quad +7092131904k^5n+514584576k^6n^2+6836900736k^3-13430568960k^4\\
&\quad -9060470784k^6+15235057152k^5-2014594176k^2+2058338304k^7)=0.
\end{aligned}
$$

Observe that – in principle – the first and second equation are sufficient to conclude. However, the Gröbner calculations become much more efficient (and faster) if one includes an additional polynomial equation.

8 Decompositions with standard pairs

8.1 Introduction

Regarding Theorem 3.1, we have to treat decompositions of $P_k^n(x)$ involving the standard pairs given by (3.4)–(3.8). Recall that by Theorem 7.2 the only non-trivial decomposition of $P_k^n(x)$ is equivalent to $P_k^n(x)=\hat{\phi}(x^2-nx)$ with $k\in 2\mathbb{Z}^+$, provided we assume the parameter restrictions for n and k given in Theorem 1.4.[5] To begin with, suppose that the Diophantine equation

$$P_k^n(x)=g(y)$$

has infinitely many rational solutions (x,y) with a bounded denominator. Then by Theorem 3.1,

$$P_k^n=\phi\circ f_1\circ\kappa_1 \qquad \text{and} \qquad g=\phi\circ g_1\circ\kappa_2,$$

where κ_1,κ_2 are some linear polynomials, $\phi\in\mathbb{Q}[x]$ and (f_1,g_1) is a standard pair as given by the list in Section 3. By Theorem 7.2, we have one of the three cases:

(i) $\deg\phi=k$,

(ii) $\deg\phi=k'$ with $k=2k'$ and $P_k^n(x)=\hat{\phi}(x^2-nx)$,

(iii) $\deg\phi=1$.

[5]Therein, we assume $k\geq 7$. It is possible to consider the smaller values of k also, however, at the cost of some more case distinctions.

8.2 Case $\deg \phi = n$

By comparison of degrees, it holds $P_k^n = \phi \circ \kappa$ for some linear polynomial $\kappa(x)$ and thus
$$g = P_k^n \circ (\kappa^{-1} \circ g_1 \circ \kappa_2) = P_k^n \circ \tilde{g}$$
for some non-constant polynomial $\tilde{g} \in \mathbb{Q}[x]$. Obviously, there are infinitely many solutions with a bounded denominator of $P_k^n(x) = P_k^n(\tilde{g}(y))$. This gives Case (i) in Theorem 1.4.

8.3 Case $\deg \phi = k$ with $k = 2k'$ and $P_k^n = \hat{\phi}(x^2 - nx)$

Let $P_k^n = \phi \circ f_1 \circ \kappa_1$ and κ be the unique linear polynomial such that $\phi \circ \kappa = \hat{\phi}$. Then $P_k^n = (\phi \circ \kappa) \circ (\kappa^{-1} \circ f_1 \circ \kappa_1) = \hat{\phi} \circ l_1$ and Theorem 7.2 yields $l_1 = x^2 - nx$. On the other hand,

$$g = \phi \circ g_1 \circ \kappa_2 = (\phi \circ \kappa) \circ (\kappa^{-1} \circ g_1 \circ \kappa_2) = \hat{\phi} \circ l_2,$$

where $l_2 = \kappa^{-1} \circ g_1 \circ \kappa_2$. If the equation $(x - n/2)^2 = l_2(y) + n^2/4$ has infinitely many solutions with a bounded denominator, then by Siegel's theorem l_2 has at most two zeroes of odd multiplicity. This yields Case (ii).

8.4 Case $\deg \phi = 1$

In this case $\phi(x) = \phi_1 x + \phi_0$ with $\phi_1, \phi_0 \in \mathbb{Q}$. Since ϕ is a linear polynomial we have to treat $P_k^n = \phi \circ f_1 \circ \kappa_1$ and $g = \phi \circ g_1 \circ \kappa_2$, where (f_1, g_1) is a standard pair with $\deg f_1 = k$. We now have to analyze all decompositions with the special polynomials of the standard pairs.

First, recall the standard pair of the *second* kind $(x^2, (\gamma x^2 + \delta) v(x)^2)$ given in (3.5). Since both $k \geq 3$ and $\deg g \geq 3$, there cannot exist a decomposition involving (f_1, g_1) of the second kind. In the same manner we can exclude the standard pair of the *fifth* kind (3.8).

Next we want to exclude decompositions with the Dickson polynomials, namely, the standard pairs of the *third* (3.6) and *fourth* kind (3.7),

$$(f_1, g_1) = (D_s(x, \gamma^t), D_t(x, \gamma^s)).$$

Assume that $P_k^n \circ \kappa = \phi \circ D_s(x, \gamma^t)$ with a linear polynomial κ, or in other words,
$$P_k^n(x) = \phi_1 D_s(\alpha x + \beta, \gamma^t) + \phi_0. \tag{8.1}$$
In view of (3.3) we here have to cope with the six variables k, n, ϕ_1, α, β and γ^t. It is again a straightforward (but involved) computation to come to a contradiction. In fact, for $k \geq 6$ we may write down six coefficient equations from (8.1) and conclude. We here omit the details.

Finally, consider the standard pair of the *first* kind given by (3.4), namely $(x^q, \gamma x^r v(x)^q)$. The polynomial $(P_k^n(x))'$ has zeroes of multiplicity one. Hence, for $k \geq 7$, there cannot be a representation with $P_k^n(\alpha x + \beta) = \phi_1 x^q + \phi_0$. On the other hand, suppose that

$$P_k^n(x) = \hat{\phi}_1(\beta_1 x + \beta_0)^r \hat{v}(x)^q + \phi_0, \tag{8.2}$$

where $\hat{\phi}_1 = \phi_1\gamma$, $\hat{v}(x) = v(\beta_1 x + \beta_0)$ with $\beta_0, \beta_1 \in \mathbb{Q}$ and $0 \leq r < q$, $\gcd(r, q) = 1$, $r + \deg \hat{v} > 0$ as demanded in (3.4). Since $q \geq 3$ by $\deg g \geq 3$, we here again come to a contradiction by arguing in the same way as above.

This concludes the investigation with linear polynomials $\phi(x)$ and finishes the proof of Theorem 1.4.

9 Summary and conclusion

In the present chapter we have outlined an analytic method to study the Diophantine equation

$$P_k^n(x) = g(y) \tag{9.1}$$

in integral variables x, y, where $P_k^n(x)$ denotes a binary Krawtchouk polynomial of degree $k \geq 7$ and $g \in \mathbb{Q}[x]$ is an arbitrary polynomial of degree ≥ 3. Within certain parameter ranges (informally speaking, k growing like $n/2$) we have shown that the Diophantine equation (9.1) only has finitely many integral solutions x, y (Theorem 1.4). This Diophantine equation is motivated by the close relationship between integrality of zeroes of Krawtchouk polynomials and the resolution of reconstruction problems in graphs (Section 3).

Our machinery ranges from a recent indecomposability criterion due to the author (Lemma 7.1) to the discrete Laguerre inequality (Theorem 4.1) applied to Krawtchouk polynomials, as obtained and outlined by Krasikov. The method used in this chapter describes a new approach in the theory of polynomial decomposition, and well fits the decomposition of discrete orthogonal polynomials. Also, the longstanding question, whether the stationary points of discrete orthogonal polynomials – or at least, a special family like the Krawtchouk polynomials – are convex, could be treated by this method. On the other hand, convexity results are well-known for the continuous orthogonal polynomial families (Laguerre, Hermite, Jacobi), but it would be a major breakthrough to show such a result for the instance of a discrete family of polynomials.

The present chapter makes this attempt for certain ranges of the degree k and the parameter $n \leq 100$ in (9.1). With more computational work it seems possible to get a general parametric result, i.e., where the result holds uniformly for all $n \geq n_0$ and $k \in I_n$, where I_n denotes a set of consecutive integers depending on n.

Acknowledgement

The author is a recipient of an APART-fellowship of the Austrian Academy of Sciences at the University of Waterloo, Canada. He wishes to express his gratitude also to I. Krasikov for several helpful discussions.

References

[1] Y. Bilu, R.F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. 95 (2000), 261–288.

[2] J.A. Bondy, *A graph reconstruction manual*, Surveys in Combinatorics, LMS-Lecture Note Series 166 (1991) (Edited by A.D. Keedwell), 221–252.

[3] A. Dujella, R.F. Tichy, *Diophantine equations for second-order recursive sequences of polynomials*, Q. J. Math 52 (2001), 161–169.

[4] M.N. Ellingham, *Vertex-switching reconstruction and folded cubes*, J. Combin. Theory Ser. B 66 (1996), 361–364.

[5] M.N. Ellingham, G.F. Royle, *Vertex-switching reconstruction of subgraph numbers and triangle-free graphs.*, J. Combin. Theory Ser. B 54 (1992), 167–177.

[6] I. Krasikov, *Applications of balance equations to vertex switching reconstruction*, J. Graph Theory 18 (1994), 217–225.

[7] I. Krasikov, *Degree conditions for vertex switching reconstruction*, Discrete Math. 160 (1996), 273–278.

[8] I. Krasikov, *Nonnegative quadratic forms and bounds on orthogonal polynomials*, J. Approx. Theory 111 (2001), 31–49.

[9] I. Krasikov, *Discrete analogues of the Laguerre inequality*, Anal. Appl. (Singap.) 1 (2003), 189–197.

[10] I. Krasikov, S. Litsyn, *On integral zeros of Krawtchouk polynomials*, J. Combin. Theory Ser. A 74 (1996), 71–99.

[11] I. Krasikov, S. Litsyn, *Survey of binary Krawtchouk polynomials*, Codes and association schemes (Piscataway, NJ, 1999), 199–211, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 56, Amer. Math. Soc., Providence, RI, 2001.

[12] I. Krasikov, Y. Roditty, *Switching reconstruction and Diophantine equations*, J. Combin. Theory Ser. B 54 (1992), 189–195.

[13] I. Krasikov, Y. Roditty, *More on vertex-switching reconstruction*, J. Combin. Theory Ser. B 60 (1994), 40–55.

[14] R. Koekoek, R.F. Swarttouw, *The Askey-Scheme of Hypergeometric Orthogonal Polynomials and its q-Analogue*, Delft, Netherlands, Report 98-17 (1998).

[15] V. Levenshtein, *Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces*, IEEE Trans. Info. Theory, 41, 1995, 1303–1321.

[16] C.L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. (1929), no. 1, 209–266.

[17] R.P. Stanley, *Reconstruction from vertex-switching*, J. Combin. Theory Ser. B 38 (1985), 132–138.

[18] T. Stoll, *Complete decomposition of Dickson-type recursive polynomials and related Diophantine equations*, J. Number Theory, 128 (2008), 1157–1181.

[19] T. Stoll, *Decomposition of perturbed Chebyshev polynomials*, J. Comp. Appl. Math. 214 (2008), 356–370.

[20] T. Stoll, R.F. Tichy, *Diophantine equations for continuous classical orthogonal polynomials*, Indagationes Math., 14 (2003), 263–274.

[21] T. Stoll, R.F. Tichy, *Diophantine equations involving general Meixner and Krawtchouk polynomials*, Quaest. Math. 28, (2005), 105–115.

[22] G. Szegő, *Orthogonal polynomials*, American Mathematical Society Colloquium Publications, vol. 23, Fourth edition, Providence, R.I., 1975.

Stoll: School of Computer Science, Faculty of Mathematics, University of Waterloo, Ontario, Canada; e-mail: `tstoll@cs.uwaterloo.ca`.