On Integral Zeros of Krawtchouk Polynomials

ILIA KRASIKOV

School of Mathematical Sciences, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel; and Beit-Berl College, Kfar-Sava, Israel

AND

SIMON LITSYN*

Department of Electrical Engineering—Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel

Communicated by the Managing Editors

Received November 4, 1993

We derive new conditions for the nonexistence of integral zeros of binary Krawtchouk polynomials. Upper bounds for the number of integral roots of Krawtchouk polynomials are presented. © 1996 Academic Press, Inc.

1. Introduction

The $q$-ary Krawtchouk polynomial $P^q_n(x)$ (of degree $k$) is defined by the following generating function:

$$
\sum_{k=0}^{\infty} P^q_n(x) z^k = (1 - z)^n (1 + (q - 1)z)^{n-x}.
$$

In the binary case ($q = 2$) it reads

$$
\sum_{k=0}^{\infty} P^2_n(x) z^k = (1 - z)^n (1 + z)^{n-x}.
$$

In what follows we consider only binary Krawtchouk polynomials. Usually $n$ is fixed, and when it does not lead to confusion it is omitted.

The question of the existence of integral zeros of Krawtchouk polynomials (or, what is essentially the same, the existence of zero coefficients in the expansion of $(1 - z)^n (1 + z)^{n-x}$) arises in many problems from combinatorics or coding theory. Let us state some of them.

* Research was supported by the Guastallo Fellowship and a grant from the Israeli Ministry of Science and Technology.
1. **Radon Transform on** $\mathbb{Z}^n_2$ [14]. Let $f : \mathbb{Z}^n_2 \to \mathbb{R}$, then the Radon transform $F_T$ of $f$ is

$$F_T(x) = \sum_{y \in T + x} f(y),$$

where $T + x$ means the set $\{t + x : t \in T\}$. The question is whether it is invertible.

2. **Switching Reconstruction Problem** [39]. Given a graph $G = G(V, E)$, $|V| = n$, for $U \subseteq V$ the switching $G_U$ of $G$ at $U$ is the graph obtained from $G$ by replacing all edges between $U$ and $V \setminus U$ by nonedges and all nonedges between $U$ and $V \setminus U$ by edges. The multiset of unlabeled graphs $D_s(G) = \{G_U : |U| = s\}$ is called the $s$-switching deck of $G$. The question is whether $G$ is uniquely defined up to isomorphism by $D_s(G)$.

3. **Reorientation Reconstruction Problem.** Given a digraph $\Gamma = \Gamma(V, E)$, $|E| = e$, that is, an orientation of edges of an ordinary graph, for any subset $A$ of $E$ denote by $\Gamma_{\hat{A}}$ the graph obtained from $\Gamma$ by the reorientation of all arcs in $A$. Define the $s$-reorientation deck $D_s(\Gamma) = \{\Gamma_{\hat{A}} : |A| = s\}$. The question again is whether $\Gamma$ is uniquely defined up to isomorphism by $D_s(\Gamma)$.

4. **Sign Reconstruction Problem.** Let $G = G(V, E)$, $|E| = e$, be a sign graph that is the graph with the edges marked by $+$ or $-$. Similarly we define the $s$-sign deck of $G$ as the multiset of signed graphs obtained from $G$ by switching signs in all the $s$-subsets of $E$. The question is the same as that above. Note that if it was permitted for $+$ signs only to be switched in the last problem then it turns out to be a generalization of the well-known edge-reconstruction problem.

5. **Perfect Binary Codes** (see, e.g., [28, 31]). Let $F^n$ be the binary Hamming space of dimension $n$. A perfect code is a set $C \subseteq F^n$ with the property that the Hamming spheres of the given radius centered at the points of $C$ cover the space $F^n$ without intersections. The question is whether such a code does exist for given $n$ and $r$.

6. **Multiple Perfect Coverings** [10, 44, 17]. A multiple perfect $s$-covering of given radius is a (multi)set $C \subseteq F^n$ with the property that the Hamming spheres of the given radius centered at the points of $C$ cover every point of the space $F^n$ precisely $s$ times. The question is whether such a covering does exist for given $s$, $n$ and $r$.

The connection of the listed problems with integral roots of Krawtchouk polynomials is reflected by the next theorem.
**Theorem 1.1.** If $P^n_s(x)$ has no integer roots then

(a) the Radon transform is invertible provided $T$ is a Hamming sphere of radius $s$ in $\mathbb{F}^n$ or a Hamming ball of radius $s$ in $\mathbb{F}^{n+1}$ [14];

(b) in Problems 3 and 4 the corresponding graphs (diagrams) are reconstructible.

2. If $P^n_s(x)$ has no even integer roots then in Problem 2 the graph is reconstructible [39].

3. If $P^n_s(x)$ has at least one noninteger root then there is no perfect code for radius $s$ in $\mathbb{F}^{n+1}$.

4. If $P^n_s(x)$ has less than $N$ integer roots then there is no perfect $\mu$-fold covering of radius $s$ in $\mathbb{F}^{n+1}$ (see [8]), where $N$ is the minimum integer such that

$$
\sum_{i=0}^{s} \binom{n}{i} \leq \mu \sum_{j=0}^{N} \binom{n}{j}.
$$

Regarding the reconstruction Problems 2–4 note that the, so called, balance equations (see [22]) for all the three problems are the same. The graphs are reconstructible if (but not only if) those equations have a unique solution. The last is true whenever the corresponding Krawtchouk polynomial (the characteristic polynomial of the matrix of the balance equations) has no integral roots. In Problem 2 only the even roots are relevant since the switching of the subset of vertices coincides with the switching of the complement subset. For perfect multiple coverings the presented condition is a particular case of a more general theorem in [8].

At present our knowledge about integral roots of Krawtchouk polynomials is quite poor. For example, in the binary case we even cannot assure in general that there is at least one nonzero root. In coding theory it was overcome by using some extra conditions, such as the sphere-packing condition. Actually [42], we know all the possibilities for parameters of binary perfect codes (see also [28, 41, 43, 45] for the corresponding results for nonbinary case, when the base equals a power of a prime). For nonbinary Krawtchouk polynomials existence of at least one noninteger root for polynomials of degree greater than 2 was proved finally by Y. Hong. His proof was based on previous works (see, e.g. [2, 3, 5]). In 1985 P. Diaconis and R. L. Graham wrote in [14]: “We do not know of any systematic study of integer zeros of Krawtchouk polynomials.” A detailed study of integral roots of binary Krawtchouk polynomials was undertaken in [9, 16]. For general properties of roots of Krawtchouk polynomials see [26, 40].

We would like to mention several questions which appear to be out of the scope of the paper but very much similar to its problematics. Namely,
they are problems of existence of perfect $L$-codes \[11, 21\], and perfect weighted coverings \[8, 12\]. In these cases we are interested in integral roots of linear combinations of Krawtchouk polynomials of different degrees.

Note that since $P_n^k(x)$ and $P_n^{n-k}(x)$ have the same sets of integral roots (see (10) below) we can and shall assume that $k \leq n/2$, unless the opposite is stated explicitly. Computer search supports the conjecture that the “typical” Krawtchouk polynomial does not have integral zeros at all, and in general can possess only a few (we conjecture 4 to be the right number) such roots. In \[16\] a list of $k$ depending on $n$ for which there exists an integral root for infinitely many $n$ is presented. Namely, such families have been found only for $k = 1, 2, 3$ and $k = (n - i)/2, i = 0, ..., 8, i \neq 7$. For other values of $k$ and $n$ only some sporadic zeros are known. It is tempting to conjecture that the known list is complete but, maybe, a small number of sporadic roots. A partial explanation for this phenomenon will be given.

In the paper we make an attempt to systematically study the existence of integral roots of Krawtchouk polynomials. We start with some relevant properties of Krawtchouk polynomials in Section 2, assemble known facts about the integral roots of Krawtchouk polynomials in Section 3, derive new upper bounds for the number of integral roots in Section 4, obtain the conditions for the existence of at least one nonintegral root in Section 5, and finally present conditions for the nonexistence of integral roots in Section 6.

2. Properties of Krawtchouk Polynomials

Here we assemble some properties of Krawtchouk polynomials. Many of them can be found in \[5, 27, 29, 31, 43\], we present them without proofs. Recall that we deal only with the binary case.

There are several explicit expressions for Krawtchouk polynomials:

\[
P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j}
\]

\[
= \sum_{j=0}^{k} (-2)^j \binom{x}{j} \binom{n-j}{k-j}
\]

\[
= \sum_{j=0}^{k} (-1)^j 2^k - j \binom{n-x}{k-j} \binom{n-k+j}{j}.
\]

\[ (2) \]
It is convenient to define \( P_k(x) = 0 \) for \( k < 0 \). A remarkable property of Krawtchouk polynomials is that in every variable they satisfy a linear recurrence relation with linear coefficients:

\[
(k + 1) \ P^\_k(x + 1) = (n - 2x) \ P^\_k(x) - (n - k + 1) \ P^\_(k - 1)(x),
\]

(notice that the relation holds also for \( k \) negative)

\[
(n - x) \ P^\_k(x + 1) = (n - 2k) \ P^\_k(x) - x P^\_(k - 1)(x - 1)
\]

(in [31] the last relation is given only for integer values of \( x \). Using Lagrange interpolation one can see that it holds as well in general, see [5]).

The following relation we did not find in literature, so we supply it with a proof.

\[
(n - k + 1) \ P^{n+1}_k(x) = (3n - 2k - 2x + 1) \ P^n_k(x) - 2(n - x) \ P^{n-1}_k(x).
\]

Proof. We start from the following easy to check identity:

\[
(n + 1)(1 - z)^n (1 + z)^{n+1-x} - z \frac{\partial}{\partial z} ((1 - z)^n (1 + z)^{n+1-x})
\]

\[
= (3n - 2x + 1)(1 - z)^n (1 + z)^{n-x} - 2z \frac{\partial}{\partial z} ((1 - z)^n (1 + z)^{n-x})
\]

\[
- 2(n - x)(1 - z)^n (1 + z)^{n-1-x}.
\]

Using (1) and comparing the coefficients at the equal powers of \( z \) we get (5).

We now list the first few Krawtchouk polynomials and some specific values:

\[
P_0(x) = 1, \quad P_1(x) = n - 2x, \quad P_2(x) = \frac{(n - 2x)^2 - n}{2},
\]

\[
P_k(0) = \binom{n}{k}, \quad P_k(1) = (1 - 2k/n) \binom{n}{k}
\]

\[
P_k(n/2) = 0, \quad \text{for } k \text{ odd;} \quad P_k(n/2) = (-1)^{k/2} \binom{n/2}{k/2}, \quad \text{for } k \text{ even.}
\]

If \( P^n_k(x) = \sum_{k=0}^k c_k x^k \) then \( c_k = (-2)^k/k! \), \( c_{k+1} = (-2)^{k+1} n/(k+1)! \). Note also that \( k! \ P^n_k(x/2) \) is a polynomial with integral coefficients.
The following relations reflect some symmetry properties of Krawtchouk polynomials with respect to their parameters:

\[
\binom{n}{x} P_n^k(x) = \binom{n}{k} P_n^x(k) \quad \text{(for nonnegative integer } x) ;
\]

\[
P_n^k(x) = (-1)^k P_n^x(n - x),
\]

\[
P_n^x(k) = (-1)^x P_n^{x-k}(x) \quad \text{(for integer } x, 0 \leq x \leq n).
\]

We would like to emphasize that \( P_n^k(x) = 0 \) for \( k < 0 \), and also for \( k > n \) if \( x \) is an integer, \( 0 \leq x \leq n \). This follows from (1) and (3).

For the Krawtchouk polynomials the following orthogonality relations hold:

\[
\sum_{i=0}^{n} \binom{n}{i} P_n^i(i) P_n^j(i) = \delta_{ij} \binom{n}{k} 2^n, \quad \sum_{i=0}^{n} P_n^i(i) P_n^j(k) = \delta_{n} 2^n.
\]

Krawtchouk polynomials satisfy the multiplication theorem, which will be presented here for less restrictive conditions than in [29]:

\[
P_n^k(x) P_n^i(x) = \sum_{j=\max(0, k+i-n)}^{\min(k, i)} a^n(k, i, j) P_n^{k+i-2j}(x),
\]

where

\[
a^n(k, i, j) = \binom{k+i-2j}{n-k-i+2j} \binom{n-k+i+j}{k+j}.
\]

**Proof.** Throughout the proof \( n \) and \( x \) are supposed to be fixed, so we omit them. First we prove that

\[
P_k P_i = \sum_{j=0}^{\min(k, i)} a(k, i, j) P_{k+i-2j}.
\]

The proof is by induction on \((k+i)\). For small values of \((k+i)\) (13) and (12) can be verified directly. Using (3) and by the induction hypothesis we have

\[
(k+1) P_{k+1} P_i = (n-2x) P_k P_i - (n+1-k) P_{k-1} P_i
\]

\[
= (n-2x) \sum_{j=0}^{\min(k, i)} a(k, i, j) P_{k+i-2j} - (n+1-k)
\]

\[
\times \sum_{j=0}^{\min(k-1, i)} a(k-1, i, j) P_{k+i-2j-1}.
\]
\[
\begin{align*}
\min(k, i) & = \sum_{j=0}^{\min(k, i)} a(k, i, j)(n - 2x) P_{k+i-j-2j} \\
& - (n+1-k-i+2j) P_{k+i-2j-1} \\
& + \sum_{j=0}^{\min(k, i)} (n + 1 - k - i + 2j) a(k, i, j) \\
& \times P_{k+i-2j+1} - (n+1-k) \\
& \times \sum_{j=0}^{\min(k-1, i)} a(k-1, i, j) P_{k+i-2j-1} \\
& = \sum_{j=0}^{\min(k, i)} a(k, i, j)(k+i-2j+1) P_{k+i-2j+1} \\
& + \sum_{j=1}^{1+\min(k, i)} a(k, i, j-1)(n-1-k-i+2j) P_{k+i-2j+1} \\
& - (n+1-k) \sum_{j=1}^{1+\min(k-1, i)} a(k-1, i, j-1) P_{k+i-2j+1}.
\end{align*}
\]

In the last expression the terms which do not appear in all three sums, sum up to zero. Also the direct calculation shows:
\[
\begin{align*}
a(k, i, j)(k+i-2j+1) + a(k, i, j-1)(n-1-k-i+2j) \\
- a(k-1, i, j-1)(n+1-k) \\
= (k+1)a(k+1, i, j).
\end{align*}
\]

Hence we get
\[
(k+1) P_{k+1} P_i = (k+1) \sum_{j=0}^{\min(k+1, i)} a(k+1, i, j) P_{k+i-2j+1}.
\]

That proves (13). To prove (12) observe that \(a(k, i, j) = 0\) whenever \(j < k + i - n\).

Now we present some known facts about zeros of Krawtchouk polynomials. \(P_n^k(x)\) has \(k\) different roots \(0 < r_{1, a}(k) < r_{2, a}(k) < \cdots r_{k, a}(k) < n\). The roots are symmetric with respect to \(n/2\), that is \(r_{i, a}(k) + r_{k+1-i, a}(k) = n\), \(i = 1, \ldots, k\). More information on location of the roots can be easily derived from the following elegant result due to V. Levenshtein [26]:
\[
r_{1, a}(k) = n/2 - \max \left( \sum_{i=0}^{k-2} x_i x_{i+1} \sqrt{(i+1)(n-i)} \right),
\]
(14)
where the maximum is taken over all \( x_i \) subjected to \( \sum_{i=0}^{k-1} x_i^2 = 1 \). Indeed, it can be assumed that all \( x_i \) are nonnegative. Particularly, we get for \( k \leq n/2 \),
\[
\begin{align*}
\quad r_{1,n}(k) & \geq n/2 - \sqrt{(k-1)(n-k+2)} \left( \sum_{i=0}^{k-2} x_i x_{i+1} \right) \\
& \geq n/2 - \sqrt{(k-1)(n-k+2)} \sqrt{\sum_{i=0}^{k-2} x_i^2 \sum_{j=1}^{k-2} x_j^2} \\
& \geq n/2 - \sqrt{(k-1)(n-k+2)}.
\end{align*}
\] (15)
Evidently, (14) enables getting other upper and lower bounds for the first root. For instance, in [27] the following estimate is given:
\[
\begin{align*}
\quad r_{1,n}(k) & \leq n/2 - \sqrt{(k(n-k)+k^{1/6})^2} \quad \text{for} \quad k \leq \lfloor n/2 \rfloor; \quad (16)
\end{align*}
\]

The roots of Krawtchouk polynomials for small \( k \) can be approximated by the corresponding roots of Hermite polynomials [2]: If \( (n-k) \to \infty \) then the zeros of \( P_n^k(x) \) approach \( n/2 + (\sqrt{n-k} - 1/2) h_1(k) \), where \( h_1(k) < \cdots < h_4(k) \) are the roots of the Hermite polynomial \( H_4(z) \).

The roots of Krawtchouk polynomials satisfy some interlacing properties (see e.g. [40, 9]), namely,
\[
\begin{align*}
\quad r_{i,n+1}(k) & < r_{i,n}(k-1) < r_{i+1,n+1}(k), \\
\quad r_{i,n}(k) & < r_{i,n+1}(k) < r_{i+1,n}(k) < r_{i+1,n+1}(k), \quad i = 1, \ldots, k-1; \quad (17)
\end{align*}
\]
Moreover, for \( i = 1, \ldots, n \), \( r_{i,n}(k) - r_{i,n+1}(k) < 1 \). For fixed \( n \) and \( k < n/2 \) (see [9]):
\[
\begin{align*}
\quad r_{i+1,n}(k) - r_{i,n}(k) > 2. \quad (18)
\end{align*}
\]

3. What Is Known About Integral Roots?

Very little is known at present about integral roots of binary Krawtchouk polynomials (without extra conditions being imposed in coding theory). To the best of our knowledge, the list of papers dealing with the problem is not very long [9, 14, 16, 23, 24]. As we have mentioned this problem can be restated via (1) and (8) as follows: How many zero coefficients does the expansion \((1-z)^n (1+z)^k\) have?

We denote by \( N(n,k)=N(k) \) the number of integral roots of \( P_n^k(x) \). The polynomial \( P_n^k(x) \) with an integer root \( r \) defines the triple \((n, k, r)\). By virtue of the relations (8)–(10) the set of these triples is closed under action of the
group of order eight generated by two involutions: \((n, k, r) \leftrightarrow (n, r, k)\) and 
\((n, k, r) \leftrightarrow (n, k, n-r)\). So, it is enough to point out representatives of the orbits.

Several infinite families of integral roots of Krawtchouk polynomials are known. Evidently, for \(n\) even and \(k\) odd we always have the integer \(n/2\) to be a root. We call such a root trivial. The known values of \(k\) for which there exists a nontrivial integer root for infinitely many \(n\) are \(k = 2, 3, (n-3)/2, (n-4)/2, (n-5)/2, (n-6)/2, (n-8)/2\), see \([9, 16]\). For \(k = 2\) and 3 it can be found from (6). For \(k\) close to \(n/2\) the following lemma is useful:

**Lemma 1.** Let \(t = n - 2k\). Then

1. \(P_k(2i) = 0 \iff \sum_{\ell=0}^{i-1} (-1)^{\ell+i} (k)_{\ell} = 0\);
2. \(P_k(2i + 1) = 0 \iff \sum_{\ell=0}^{i-1} (-1)^{\ell+i+1} (k)_{\ell} = 0\).

**Proof.** Using (8) and (1) one can see that to find the even and odd zeros of \(P_k(x)\) one should find zero coefficients with even and odd indices respectively of \((1-z)^k (1+z)^{n-k} = (1-z^2)^k (1+z)^{n}\). Now the result follows from calculating the coefficient at \(z^{2i}\) and \(z^{2i+1}\) respectively.

The lemma yields that the nontrivial roots can be found from the following equations (for \(t > 3\) reducing to Pell equations):

1. \(t = 3\): \(r = (n-1)/4\) (even roots); \(t = 3\): \(r = (3n+1)/4\) (odd roots);
2. \(t = 4\): \(8r^2 - 8nr + n^2 - 2n = 0\) (even roots);
3. \(t = 5\): \(16r^2 - 12nr + 4r + n^2 - 4n + 3 = 0\) (even roots); \(16r^2 - 20nr - 4r + 5n^2 + 3 = 0\) (odd roots);
4. \(t = 6\): \(16r^2 - 16nr + n^2 - 6n + 8 = 0\) (even roots); \(16r^2 - 16nr + 3n^2 - 2n + 8 = 0\) (odd roots);
5. \(t = 8\): \(8r^2 - 8nr + n^2 - 2n + 16 = 0\) (odd roots).

For other values of \(t\) we get either only the trivial root or a diophantine equation of degree greater than two. Here is the list of sporadic roots for \(n < 8400\) (we hope it is complete in the range):

\[
\begin{array}{ccccccccc}
k & 5 & 4 & 5 & 5 & 6 & 23 & 14 & 19 & 61 & 31 & 5 & 44 & 34 \\
r & 14 & 30 & 22 & 28 & 31 & 31 & 47 & 62 & 86 & 103 & 133 & 155 & 230 & 254 \\
\end{array}
\]

\[
\begin{array}{ccccccccccccc}
n & 576 & 774 & 932 & 1029 & 1219 & 1219 & 1252 & 1521 & 3193 & 3362 & 4516 & 4712 & 7302 & 8361 \\
k & 84 & 113 & 62 & 7 & 116 & 421 & 183 & 4 & 1103 & 492 & 661 & 480 & 1069 & 798 \\
r & 286 & 383 & 463 & 496 & 607 & 607 & 622 & 715 & 1594 & 1679 & 2254 & 3583 & 3647 & 4178 \\
\end{array}
\]
Observe that in all cases for which an infinite family was presented either $k < 8$ or $t < 9$. It is also valid for the infinite families presented earlier. A partial explanation of this phenomenon is given in the following three theorems.

**Theorem 2 [23].** For fixed $k \geq 4$, $P_n^k(x)$ can have nontrivial integer roots only for finitely many $n$.

**Theorem 3 [24].** Let $t > 6$ be either an odd prime, a power of 2 or of the form $2pq$, where $p$ is an odd prime, $q$ is odd, and $p$ does not divide $q$. Then for $k = (n - t)/2$, $P_n^k(x)$ can possess nontrivial even roots only for finitely many $n$.

Define the polynomials

$$V_t(x, y) = \sum_{j=0}^{[t/2]} (-1)^j \binom{t}{2j} \prod_{i=0}^{j-1} (x - i) \prod_{i=0}^{[t/2]-j-1} (y - i),$$

$$V_t^*(x, y) = V_t(x, y) \text{ for } t \not\equiv 2 \pmod{4}, \text{ and } V_t(x, y)/(x - y) \text{ otherwise},$$

$$U_t(x, y) = \sum_{j=0}^{[(t-1)/2]} (-1)^j \binom{t}{2j+1} \prod_{i=0}^{j-1} (x - i) \prod_{i=0}^{[(t-1)/2]-j-1} (y - i),$$

$$U_t^*(x, y) = U_t(x, y) \text{ for } t \not\equiv 0 \pmod{4}, \text{ and } U_t(x, y)/(x - y) \text{ otherwise}.$$

**Theorem 4 [24].** Let $k = (n - t)/2$, $t$ fixed. There are at most finitely many $n$ such that $P_n^k(x)$ has an even nontrivial root provided $t < 7$ whenever $V_t^*(x, y)$ is irreducible over $\mathbb{Z}[x, y]$; and $P_n^k(x)$ has an odd nontrivial root provided $t = 7$ or $t \geq 9$ whenever $U_t^*(x, y)$ is irreducible over $\mathbb{Z}[x, y]$.

**Proof.** Multiplying the expressions from Lemma 1 by $i!y!/k!$, where $y = (k + [t/2] - i)$ for the even case and $y = (k + [(t-1)/2] - i)$ for the odd case, and putting $x = i$, we get that $P_n^k(2i) = 0$ iff $V_t(i, y) = 0$ and $P_n^k(2i+1) = 0$ iff $U_t(i, y) = 0$. Observe also that by the symmetry of $V_t(x, y)$ in $x$ and $y$ for $t \equiv 2 \pmod{4}$, $x - y$ is a factor of $V_t(x, y)$ and gives the trivial root. Similarly, for $t \equiv 0 \pmod{4}$, $x - y$ is a factor of $U_t(x, y)$ and gives the trivial root. Now the claim follows from the Runge theorem [32, 34] (the extra condition—the polynomial is not a constant multiple of a power of an irreducible polynomial—can be easily checked).

Let us make some remarks on effectivity of the three theorems above. Theorems 2 and 3 are based on a result due to A. Shinzel [35] which does not provide an effective upper bound on $n$. However, for the cases $k = 4, 5$, one can use an effective version of Siegel’s theorem [38] due to A. Baker.
As usual the bounds occur to be enormously large. For these cases the equations get the form:

\[ k = 4; \quad 3n^2 - 6n(n - 2r)^2 + 1 + (n - 2r)^4 + 8(n - 2r)^2 = 0, \]

\[ k = 5; \quad 15n^2 - 10n(n - 2r)^2 + 5 + (n - 2r)^4 + 20(n - 2r)^2 + 24 = 0. \]

For the case \( k = 4 \) the following solutions \((n, r), n > 8 \) and \( r < n/2 \) satisfy the equation: \((17, 7), (66, 30), (1521, 715), (15043, 7476)\) [14]. This case was studied in [16]. For \( k = 5, n > 10 \), the list of solutions is \((17, 3), (36, 14), (67, 22), (67, 28), (289, 133), (10882, 5292)\). Both lists are conjectured to be complete. Note also that, as it was pointed out in [14], for \( k = 4 \) (it is valid as well for \( k = 5 \)) the above diophantine equations possess infinitely many rational solutions.

The third theorem is based on the Runge theorem (for our purposes it is enough to use a special case presented in [32]). Effective bounds for this case were derived in [19, 20]. Irreducibility of \( V_t^*(x, y) \) and \( U_t^*(x, y) \) for small \( t \) could be checked directly. We conjecture that actually they are always irreducible. Of course, for \( k \) and \( t \) depending on \( n \) this method is not applicable. We finish the section with some conjectures.

**Conjecture 1 [9]**. Let \( k > 3 \) or \( t > 6, t \neq 8 \). Then the number of non-trivial integer zeros of \( P_n^k(x) \) for \( n < \cdot \) is \( o(\cdot) \).

**Conjecture 2**. For \( 3 < k < n/2 \), any Krawtchouk polynomial possesses a noninteger root.

**Conjecture 3**. For \( k < n/2 \) there exists an absolute constant \( c \) such that \( N(k) \leq c \). That is, the number of zero coefficients in the expansion \((1 - z)^i (1 + z)^j, i < j \), does not exceed \( c \).

Actually, according to numerical evidence we guess \( c \) to be 4 for \( n \) even, and 3 for \( n \) odd. In this context it is worth mentioning [25, 6] where it was proven that the number of zeros arising from binary nondegenerated recurrences with integer constant coefficients does not exceed 4 (see also [7, 33]). Unfortunately, in our case the recursion turns out to be with linear coefficients.

The following particular case of the above conjecture is of some importance for switching reconstruction.

**Conjecture 4 [24]**. The only integer zeros of \( P_n^k(x) \), \( k = (\frac{m^2}{n}), n = m^2 \), are \( 2, m^2 - 2 \), and, \( m^2/2 \) for \( m \equiv 2 \) (mod 4).
4. How Many Integral Roots Can Occur?

In this section we derive some bounds for the number of integral roots of Krawtchouk polynomials. We start with the following simple

**Theorem 5.**

\[ N(k) \leq \min(k, n - 2k). \]

**Proof.** Notice that \( \deg P_n^k(x) = k \), and the degrees of \( U_i(x, y) \) and \( V_i(x, y) \) in \( x \) are at most \( \lceil (t - 1)/2 \rceil, \lceil t/2 \rceil \), respectively, \( t = n - 2k \). From the proof of Theorem 4 we have that:

\[ P_n^k(2i) = 0 \quad \text{iff} \quad V_i(i, k + \lceil t/2 \rceil - i) = 0 \]

and

\[ P_n^k(2i + 1) = 0 \quad \text{iff} \quad U_i(i, k + \lceil (t - 1)/2 \rceil - i) = 0 \]

The result follows now from Lemma 1 since

\[ \deg(V_i(i, k + \lceil t/2 \rceil - i)) + \deg(U_i(i, k + \lceil (t - 1)/2 \rceil - i)) = \lceil (t - 1)/2 \rceil + \lceil t/2 \rceil \leq n - 2k. \]

For convenience we use change of variable \( y = n - 2x \), defining \( Q_k(y) = P_k((n - y)/2) \). Let \( y_i, i = 1, \ldots, k \), be its roots. Notice that they are symmetric with respect to zero.

\[ Q_k(y) = \begin{cases} \left( \prod_{i=1}^{k/2} (y^2 - y_i^2) \right) & k \text{ even} \\ \left( \prod_{i=1}^{\lfloor k/2 \rfloor} (y^2 - y_i^2) \right) & k \text{ odd} \end{cases} \]  

(19)

Note also, that if \( P_k(x_i) = 0 \) and \( x_i \) is integral then

\[ y_i \equiv n \pmod{2}. \]  

(20)

Here are a few values of \( Q_k(y) \) for small \( y \)’s:

\[ Q_{2k}(0) = (-1)^{k - 1} \frac{k}{(2k)!} \prod_{i=0}^{k-1} (n - 2i); \quad Q_{2k+1}(0) = 0; \]  

(21)

\[ Q_{2k}(1) = (-1)^{k - 1} \frac{k}{(2k)!} \prod_{i=0}^{k-1} (n - 2i - 1); \]

\[ Q_{2k+1}(1) = (-1)^{k - 1} \frac{k}{(2k)!} \prod_{i=0}^{k-1} (n - 2i - 1); \]  

(22)
\[ Q_{2k}(2) = \frac{(-1)^k}{(2k)!} (n-4k) \prod_{i=1}^{k-1} (n-2i); \]
\[ Q_{2k+1}(2) = 2 \frac{(-1)^k}{(2k)!} \prod_{i=1}^{k} (n-2i); \] (23)
\[ Q_{2k}(3) = \frac{(-1)^k}{(2k)!} (n-8k-1) \prod_{i=1}^{k-1} (n-2i-1); \]
\[ Q_{2k+1}(3) = \frac{(-1)^k}{(2k)!} (3n-8k-3) \prod_{i=1}^{k-1} (n-2i-1); \] (24)

In general, we have

**Lemma 2.** For integer \( y < 2k \), the following relations hold:

\[ Q_{2k}(y) = (-1)^k \frac{F_y(k, n)}{(2k)!} \prod_{i=0}^{k-1} (n-y-2i); \] (25)
\[ Q_{2k+1}(y) = (-1)^k \frac{G_y(k, n)}{(2k)!} \prod_{i=0}^{k-1} (n-y-2i); \] (26)

where \( F_j(k, n) \) and \( G_j(k, n) \) for fixed \( j \) are polynomials in \( k \) and \( n \), with integer coefficients. For \( n \) growing, \( n \to \infty \), and \( k = o(\sqrt{n}) \),

\[ F_j(k, n) = n^{(j/2)}(1 + o(1)), \quad G_j(k, n) = n^{j-1}(1 + o(1)), \] (27)
\[ G_{2j+1}(k, n) = (2j+1) n^j (1 + o(1)), \]

and for \( k = o(n) \),

\[ F_j(k, n) < n^{(j/2)}(1 + o(1)), \quad G_j(k, n) < n^{j-1}(1 + o(1)), \]
\[ G_{2j+1}(k, n) < (2j+1) n^j (1 + o(1)). \] (28)

*Proof.* Using (1) one easily gets that the above relations hold for \( y = 0, 1, 2, 3, 4 \). The proof is accomplished by induction on \( y \). We will demonstrate it for \( Q_{2k}(2y) \).

Rewriting (4) in terms of \( Q_{2k}(y) \) and \( y \) we get:

\[(n-y) Q_{2k}(y+2) = 2(n-2k) Q_{2k}(y) - (n+y) Q_{2k}(y-2). \]
Substitution of $k$ by $2k$ and of $y$ by $2y$ yields:

$$(n - 2y) Q_{2y}\neq (2y + 2) = 2(n - 4k) Q_{2y} - (n + 2y) Q_{2y} (2y - 2).$$

By induction (omitting the common factor $(-1)^k/(2k)!$) we get

$$(n - 2y) F_{2y+2}(k, n) \prod_{i=0}^{k-y-2} (n - 2y - 2 - 2i) = 2(n - 4k) F_{2y}(k, n) \prod_{i=0}^{k-y-1} (n - 2y - 2i) - (n + 2y) F_{2y-2}(k, n) \prod_{i=0}^{k-y} (n - 2y + 2 - 2i).$$

After cancellation we obtain

$$F_{2y+2}(k, n) = 2(n - 4k) F_{2y}(k, n) - (n + 2y)(n - 2y + 2) F_{2y-2}(k, n),$$

that proves the claim. For the other cases the proof is similar.

To prove (27) and (28) observe that by induction on $y$ we get:

$$F_{2y+2} = n^{r+1}(1 - O(k/n))^r,$$

thus giving the claimed asymptotics.

Define for $a$ integer the function $E(a)$ as the maximum power of 2 dividing $a$.

**Theorem 6.1.** For $k$ and $n$ even $N(k) \leq \frac{1}{16} (5k + 4E(n/2 - k) + 6E((n/2 - 1)!/(n - k)/2)!)$;

2. For $k$ odd and $n$ even $N(k) \leq \frac{1}{16} (5k + 11 + 4E(n/2 - 1) + 6E(n/2 - k) + 10E((n/2 - 1)!/(n - k)/2)!)$.

3. For $k$ even and $n$ odd $N(k) \leq \frac{1}{4}(k + 2E(((n - 1)/2)!/(n - k)/2)!)$.

4. For $k$ and $n$ odd $N(k) \leq \frac{1}{4}(k - 1 + 2E(((n - 1)/2)!/(n - k)/2)!)$.

**Proof.** We give a complete proof only for the first case. In the other cases the arguments are analogous. We put $n = 2m$ and $k = 2l$. Furthermore, let $P_n(x)$ have $2s$ integral roots $\pm 2v_i, i = 1, ..., s$ (recall that $v_i$ is integer by (20)). Then from (19)

$$(2l)! Q_{2l}(y) = \prod_{i=1}^{s} (y^2 - 4v_i^2) R(y),$$
where $R(y)$ is a polynomial with integer coefficients. Now:

$$(2l)! \cdot Q_{2l}(0) = (-1)^s R(0) \prod_{i=1}^{s} 4v_i^2 = (-1)^{s} \frac{(2l)!}{(2l)!} \prod_{i=0}^{l-1} (2m-2i), \quad (29)$$

$$(2l)! \cdot Q_{2l}(2) = R(2) \prod_{i=1}^{s} (4 - 4v_i^2) = (-1)^s \frac{(2l)!}{(2l)!} \prod_{i=1}^{l-1} (2m-2i), \quad (30)$$

Multiply the cube of (29) by the square of (30), and estimate the maximum power of 2 dividing the LHS and the RHS (in what follows, denoted by $E(\text{LHS})$ and $E(\text{RHS})$):

$$E(\text{RHS}) = 3(l + E((m)!)) - E((m-l)!) + 2(l + E(m-2l))$$

$$+ E((m-1)!) - E((m-l)!))$$

$$= 5l + 3E(m) + 2E(m-2l) + 5E((m-1)!)) - 5E((m-l)!).$$

For the LHS we have

$$E(\text{LHS}) \geq E \left( (2^n)^3 \prod_{i=1}^{s} v_i^6 \left( (2^n)^2 \prod_{i=1}^{s} (1 - v_i^2)^2 \right) \right)$$

$$= 10s + E \left( \prod_{i=1}^{s} v_i^6 (1 - v_i^2)^2 \right).$$

Note that $a^6(1 - a^2) \equiv 0 \pmod{2^6}$ hence $E(\text{LHS}) \geq 16s$, and the sought result follows. In other cases we consider correspondingly $(Q_k(2))^2$, $(Q_k(4))^3$, $Q_k(1)$ $Q_k(3)$ and $Q_k(1)$ $Q_k(3)$. $\blacksquare$

**Corollary 1.**

1. For $k$ and $n$ even $N(k) \leq ((5k - 13)/8) + \log_2 n + 4\log_2 k$;

2. For $k$ odd and $n$ even $N(k) \leq ((5k - 10)/8) + \log_2 n + \frac{1}{4}\log_2 k$;

3. For $k$ even and $n$ odd $N(k) \leq ((4k - 8)/7) + \frac{1}{4}\log_2 n + \frac{1}{2}\log_2 k$;

4. For $k$ and $n$ odd $N(k) \leq ((4k + 6)/7) + \frac{1}{2}\log_2 n + \frac{1}{4}\log_2 k$.

**Proof.** We use the inequalities

$$E(a) \leq [\log_2 a], \quad a - [\log_2 a] - 1 \leq E(a!) \leq a - 1. \quad (31)$$

The inequalities on $E(a!)$ follow from

$$E(a!) = \sum_{i=1}^{[\log_2 a]} \left[ \frac{a}{2^i} \right],$$
by
\[
\sum_{i=1}^{[\log_2 a]} \left( \frac{a}{2^i} - 1 \right) \leq E(d) \leq \sum_{i=1}^{[\log_2 a]} \frac{a}{2^i}.
\]

We will prove here only the first case of the corollary. The three others are similar. First we estimate
\[
E^* = 2E \left( \frac{n}{2} - k \right) + 3E \left( \frac{n}{2} \right).
\]

Observe, that \( \text{GCD}((n/2) - k, n/2) \leq k \). That yields
\[
E \left( \frac{n}{2} - k \right) + E \left( \frac{n}{2} \right) \leq [\log_2 k] + \max \left( E \left( \frac{n}{2} - k \right), E \left( \frac{n}{2} \right) \right).
\]

Since we have that
\[
E \left( \frac{n}{2} - k \right) \leq \left[ \log_2 \left( \frac{n}{2} - k \right) \right] \leq \left[ \log_2 \left( \frac{n}{2} \right) \right] \quad \text{and} \quad E \left( \frac{n}{2} \right) \leq \left[ \log_2 \left( \frac{n}{2} \right) \right],
\]

we can conclude that
\[
\max \left( E \left( \frac{n}{2} - k \right), E \left( \frac{n}{2} \right) \right) \leq \log_2 \left( \frac{n}{2} \right).
\]

Now:
\[
E^* = 2E \left( \frac{n}{2} - k \right) + 3E \left( \frac{n}{2} \right) = 2 \left( E \left( \frac{n}{2} - k \right) + E \left( \frac{n}{2} \right) \right) + E \left( \frac{n}{2} \right)
\]
\[
\leq 2 \left( [\log_2 k] + \max \left( E \left( \frac{n}{2} - k \right), E \left( \frac{n}{2} \right) \right) \right) + E \left( \frac{n}{2} \right)
\]
\[
\leq 2 [\log_2 k] + 3 [\log_2 (n/2)].
\]

Routine calculations lead now to the result.

The theorem states that for sufficiently large degrees \( k \) of Krawtchouk polynomials \( (k/(\log n) \to \infty) \) the number of integer roots does not exceed 5/8 of the total amount. This coefficient may be improved in expense of the coefficient at \( \log n \) using products of more than two values of \( Q_i(k) \). Actually, we did not try to get the best possible bound achievable by this method since it does not seem possible to get the coefficient at \( k \) less than 0.5.
**Theorem 7.** If \( k = o(n) \), then

1. for \( k \) and \( n \) even, and any \( \theta = 2^l \leq (k/2) - 1 \)

\[
N(k) < \frac{2\theta + 2}{4\theta + 1} k + \frac{\theta}{4} \log_2 n + o(\theta \log n) \leq \frac{k}{2} + \frac{3}{8} k \log_2 n + o(\sqrt{k \log n}); \quad (32)
\]

2. for \( k \) odd and \( n \) even, and any \( \theta = 2^l \leq k/2 \)

\[
N(k) < \frac{\theta}{2\theta - 1} k + \frac{\theta}{4} \log_2 n + o(\theta \log n) \leq \frac{k}{2} + \frac{1}{2} \sqrt{k \log_2 n} + o(\sqrt{k \log n}); \quad (33)
\]

3. for \( n \) odd, and any \( \theta = 2^l - 1 \leq [k/2] \)

\[
N(k) < \frac{\theta + 1}{2\theta + 1} k + \frac{\theta}{4} \log_2 n + o(\theta \log n) \leq \frac{k}{2} + \frac{1}{2} \sqrt{k \log_2 n} + o(\sqrt{k \log n}). \quad (34)
\]

**Proof.** We will prove the theorem for the case \( n = 2m + 1, k = 2l + 1 \). The other cases are similar. Let \( 2v_i + 1, i = 1, \ldots, s \), be integer roots of \( Q^*(y) \) corresponding to the integral roots of \( P^*(x) \). Then from (19) and (28)

\[
(2l + 1)! Q_{2l + 1}(2z + 1) = (2z + 1) A(z) R(2z + 1) = (-1)^l \frac{(2l + 1)!}{(2l)!} (2z + 1) B(z), \quad (35)
\]

where

\[
A(z) = \prod_{i=1}^s ((2z + 1)^2 - (2v_i + 1)^2),
\]

\[
B(z) = G_{2z + 1}(l, n) \prod_{i=z}^{l-1} (2m - 2i).
\]

Pick some integer \( \theta \) of the form \( 2^l - 1 \leq l - 1 \), and consider \( A^*(\theta) = \prod_{z=0}^\theta A(z) \) and \( B^*(\theta) = \prod_{z=0}^\theta B(z) \). Observe

\[
A^*(\theta) = 2^{2\theta(\theta + 1)} \prod_{i=1}^\theta \prod_{z=0}^\theta (v_i - z)(v_i + z + 1).
\]

Evidently,

\[
E\left( \prod_{z=0}^\theta (v_i - z)(v_i + z + 1) \right) \geq E((2\theta + 2)!)) = 2\theta + 1,
\]
thus

\[ E(A^*(\theta)) \geq 2s(\theta + 1) + sE((2\theta + 2)!)] \geq s(4\theta + 2). \]

Further,

\[
E(B^*(\theta)) = \sum_{z=0}^{\theta} E(B(z)) = \sum_{z=0}^{\theta} E(G_{2z+1}(l, n)) + \sum_{z=0}^{\theta} E\left(\prod_{i=0}^{l-1} (2m-2i)\right)
\]

\[ \leq \sum_{z=0}^{\theta} \log_2(G_{2z+1}(l, n)) + \sum_{z=0}^{\theta} E\left(\prod_{i=0}^{l-1} (2m-2i)\right) \leq (\text{by (28)}) \]

\[
\sum_{z=0}^{\theta} \log_2(n^i(1+o(1))) + (\theta + 1)\left(I + E\left(\frac{m!}{(m-l)!}\right)\right)
\]

\[ \leq \sum_{z=0}^{\theta} \log_2(n\log_2(1+o(1)) + (\theta + 1)(l + \log_2 m)
\]

\[ \leq (\theta + 1)\theta \left(\log_2 n + o(1)\right) + 2(\theta + 1) + (\theta + 1)\left(\log_2 \frac{n-1}{2}\right).
\]

Hence, from \(E(A^*(\theta)) \leq E(B^*(\theta))\) follows

\[ s \leq \frac{(\theta + 1)(\theta + 2)}{8\theta + 4} \log_2 n + \frac{\theta + 1}{2\theta + 1} l - \frac{\theta + 1}{4\theta + 2} + o\left(\frac{(\theta + 1)\theta}{4\theta + 2}\right)
\]

\[ \leq \frac{\theta + 1}{2\theta + 1} l + \frac{\theta}{8} \log_2 n + o(\theta \log_2 n).
\]

Recalling that the number of integer roots equals \(2s + 1\) for this case, we conclude that it does not exceed

\[ \frac{\theta + 1}{2\theta + 1} k + \frac{\theta}{4} \log_2 n + o(\theta \log n).
\]

Choosing \(\theta\) to be about \(\sqrt{k/\log_2 n}\) we get the last inequality in (34). \]

For \(k\) growing faster than \(\sqrt{n}\) we will derive bounds based on other ideas.

**Theorem 8.**

\[ N(k) \leq \frac{3}{2} \sqrt{2(k-1)(n-k+2)}. \]
Proof. We start by showing that the number of pairs of integer roots at distance $i$ apart can not be too large. Let $r < n/2$ be an integer root of $P_k(x)$. Then, by (18), $r + 1$ is not a root. Define

$$S(x) = \frac{(n - r - 1)! P_k(r + x)}{(n - r)! P_k(r + 1)}.$$  

By (4) $S(x)$ satisfies the following recurrence with $S(0) = 0$, $S(1) = 1$:

$$S(x + 1) = (n - 2k - r) S(x) - (n - r - x + 1) S(x + 1).$$

This recurrence shows that for integer $x$, $S(x)$ can be considered to be a polynomial in $r$ of degree

$$d(x) = \deg S(x) \leq \begin{cases} x - 2 & \text{if } x \text{ even;} \\ x - 1 & \text{if } x \text{ odd.} \end{cases}$$

Thus the number of integer roots $r$, such that there is another integer root at distance $x$ from $r$, does not exceed $d(x)$. Hence, we may remove from the set of integer roots not more than $(d(x) + 1)/2$ elements so that the distance $x$ does not appear in the resulting set. Let $L$ denote $r_d(k) - r_s(k)$. From (15), $L < \sqrt{(k - 1)(n - k + 2)}$. Now remove

$$\sum_{i=3}^{h+1} \frac{d(i) + 1}{2} < \frac{1}{2} \sum_{i=3}^{h-1} i < \frac{1}{2} \left( \binom{h}{2} - 1 \right)$$

roots so that in the resulting set the minimum distance is at least $h$. The minimum length of an interval covering this set is at least $(N(k) - \frac{1}{2}(h)) h < L$. Choosing $h$ to be $(2L)^{1/3}$ we obtain the claim.  

**Corollary 2.** $N(k) \leq (\frac{2}{9} n)^{2/3}$.

5. **WHEN DOES THERE EXIST AT LEAST ONE NONINTEGER ROOT?**

The question in the section’s title is crucial for proofs of nonexistence of perfect codes. The problem is far from being trivial. A significant effort has been made to achieve the goal. For the nonbinary case ($q \neq 2$) nonsymmetry of Krawtchouk polynomials with respect to $(q - 1)/n$ was essentially exploited [2, 5, 18], see also [28, 41, 45]. In the binary case $P_n^q(x)$ is symmetric with respect to $n/2$ so the mentioned approach fails to work. A. Tietäväinen [42] overcame it using the sphere-packing condition. Thus for the binary case the question is still open.
First observe that if \( n \) and \( k \) are odd then \( n/2 \) is such a root. Furthermore, an immediate consequence of Theorem 6 and Corollary 1 is

**Theorem 9.** There exists a constant \( c \) such that for \( k > c \log n \), \( P_n^k(x) \) has a noninteger root.

For example for \( n > 22 \) one may choose \( c = 3 \). Now we will use a particular case of a result due to T. N. Shorey and R. Tijdeman [37]:

**Theorem 10 [37].** Let \( \varepsilon > 0 \) and \( m > j^2 \), \( A(m, j, d) = m(m - d)(m - 2d) \cdots (m - (j - 1) d) \). Then there exists an effectively computable number \( c \) depending only on \( \varepsilon \) and \( d \) such that for \( k > c \) one can find a prime \( p > (1 - \varepsilon) k \log \log k \) for \( d = 1 \) and \( p > (1 - \varepsilon) k \log \log \log k \) otherwise, with a property that for some nonnegative integer \( l \), \( p^{2l+1} \mid A(m, j, d) \) and \( p^{2l+2} \mid A(m, j, d) \).

This theorem guarantees that under suitable conditions \( A(m, j, d) \) can not be a perfect square. It is used to obtain the following

**Theorem 11.** For \( k \) even and sufficiently large (effectively computable and independent on \( n \)), \( P_n^k(x) \) has a noninteger root.

**Proof.** By Corollary 1 we may assume that \( k = o(\sqrt{n}) \).

Consider \( Q_k(0) \) defined in (21). Assuming by the contrary that all the roots \( y_1, \ldots, y_k, \) of \( Q_k(y) \) are integer we have for \( n \) odd:

\[
(-1)^{k/2} k! Q_k(0) = k! \prod_{i=b}^{k-1} (n - 2i) = \prod_{i=1}^{k/2} y_i^2.
\]

Applying Theorem 10 with \( d = 2 \), \( m = n \) and \( j = k/2 \), we get that the LHS has a prime factor of odd order and greater than \( k \), thus contradicting the RHS is a perfect square.

Similarly, for \( n \) even we have:

\[
(-1)^{k/2} k! Q_k(0) = \binom{n/2}{k/2} k! \prod_{i=1}^{k/2} y_i^2.
\]

This yields that the number

\[
\frac{k!}{(k/2)! (n/2)! (n - k/2)!}
\]

is a perfect square. Again Theorem 10 with \( d = 1 \), \( m = n/2 \) and \( j = k/2 \), shows that this is impossible. \( \square \)
Since for \( n \) and \( k \) odd \( n/2 \) is a noninteger root, we get:

**Corollary 3.** For \( n \) odd and \( k \) sufficiently large \( P_n^k(x) \) always has a noninteger root.

The case \( n \) even and \( k \) odd turns out the most difficult (at least for us). In this case \( Q_k(0) = 0 \), but one may consider its derivative:

\[
k! Q_k(0) = \sum_{i=0}^{(k-1)/2} (-1)^i \left( \begin{array}{c} n/2 \\ i \end{array} \right) \frac{k!}{k-2i},
\]

that is obligatory a perfect square if all the roots are integer. Although we conjecture it is never the case we failed to prove it. For this situation (as well as for the cases having considered in Theorem 11, but now for all \( k \)'s) we give some partial results using another method.

The following expressions for sums of powers of roots of \( Q_k(y) \) prove to be useful:

\[
\sum_{i=1}^{k} y_i^2 = \frac{1}{2} k(k-1)(3n-2k+4); \tag{36}
\]

\[
\sum_{i=1}^{k} y_i^6 = \frac{1}{4} k(k-1)(105n^3k^2 - 357n^3k + 315n^3

- 252n^2k^3 + 1449n^2k^2 - 2835nk^3 + 1890nk^2 + 210nk^4 - 1680nk^3 + 5082nk^2 - 6888nk + 3528n - 60k^5 + 612k^4 - 2496k^3 + 5064k^2 - 5072k + 1984). \tag{37}
\]

To derive these expressions it is sufficient calculating the seven first coefficients \( a_0, \ldots, a_6 \) (starting from the leading one) of \( Q_k(y) \), and then using the Newton formula for \( i = 1, \ldots, k \):

\[
a_i + \sum_{j=0}^{i-1} a_j \sum_{l=1}^{k} y_l^{i-j} = 0.
\]

We have used the Mathematica package to fulfill the calculations.

**Theorem 12.** For \( n \equiv 0 \pmod{4} \) and \( k \equiv 3 \pmod{4} \), or \( n \equiv k \equiv 2 \pmod{4} \), or \( n \equiv 6 \pmod{8} \) and \( k \equiv 4 \pmod{8} \), or \( n \equiv 0 \pmod{8} \) and \( k \equiv 5 \pmod{8} \), \( P_n^k(x) \) possesses an noninteger root.

**Proof.** Recall that if all the roots are integral then for \( n \) even all \( y_i \)'s are also even. Now consider \( \sum_{i=1}^{k} y_i^2 \). Then \( y_i^2 \equiv 0 \pmod{4} \). Since the roots are symmetric with respect to zero the sum is divisible by 8. Checking divisibility by 8 of the RHS of (36) we get the first two items. The other
two (as well as the first two) can be derived in the same fashion from (37).

Other conditions could be derived from considering of $Q_{2a}(0)$ and $Q_{2a+1}(2)$.

**Theorem 13.**
1. If for $n$ and $k$ both even, $k < \sqrt{n/2}$, there exists a prime $p \geq \sqrt{n/2}$, dividing one of the integers in the interval $[(n-k)/2+1, n/2]$ then $P_n(x)$ possesses an noninteger root;

2. If for $n$ even and $k$ odd there exists a prime $p \geq (k-1)(n-k+2)+2$ dividing one of the integers in the interval $[(n-k+1)/2, (n/2)-1]$ then $P_n(x)$ possesses an noninteger root.

**Proof.** In the first case consider

$$k! \; Q_k(0) = (-2)^{k/2} \frac{k!}{k!} \prod_{i=0}^{k/2-1} (n/2-i) = (-1)^{k/2} \prod_{i=1}^{k/2} y_i^2,$$

here $k$ is even and assume all $y_i$ are integers. Suppose that the announced prime $p$ does exist. Then $p^2$ must divide the RHS. Since at most one of the integers in the interval is divisible by $p$ this one must be divisible by $p^2$ as well. Hence, $p^2 \leq n/2$, a contradiction.

In the second case we consider $Q_k(2)$. As above we see that $p$ must divide either $(y_i/2-1)$ or $(y_i/2+1)$ for some $i$. But from (15) we get that $|y_i/2+1| < \sqrt{(k-1)(n-k+2)+1}$.

Now we apply Theorem 6 to establish the existence of a noninteger root for the case when the interval $[(n-k)/2, n/2]$ does not contain numbers divisible by too large powers of 2.

We extend the definition of function $E(a)$ equal to the maximum degree of 2 dividing $a$ to an arbitrary set $A$ of integers by setting $E(A) = \max_{a \in A} E(a)$. If $A$ is an interval then $E(\prod_{a \in A} a)$ can be easily upper-bounded in terms of $E(A)$.

**Lemma 3.** Let $A = [a, b]$, then $E(b!/(a-1)!) \leq b - a + 1 + E(A)$.

**Proof.** The number of integers in $A$ divisible by $2^i$ does not exceed $(b-a+1+2^{i-1})/2^i$. Summing up by $i$ from 1 to $E(A)$ and taking the integer part we get the claim.

**Theorem 14.** $P_n(x)$ has an noninteger root if

1. $n$ and $k > 8$ even, and $E(\{(n/2)\} - k) \cup [(n-k)/2, (n/2)-1]) \leq \frac{3}{4} k - \log_2 k + \frac{16}{a}$,

2. $n$ even and $k > 18$ odd, and $E(\{(n/2)\} - k) \cup [(n-k+1)/2, (n/2)-1]) \leq \frac{3}{4} k - \log_2 k + 4$. 


Proof. We give a proof for the second case, the first can be proved similarly. Put \( u = (E((n/2) - k) \cup [(n - k + 1)/2, (n/2) - 1]) \). We consider three subcases:

1. \( 2^n | a, \ a \in A = [(n - k + 1)/2, (n/2) - 1] \). Since \( \forall b \in A \ GCD((n/2) - 1, b) \leq (k - 3)/2 \) and \( GCD((n/2) - k, b) \leq k - 2 \), then \( E((n/2) - 1) \leq \log_2(k - 3)/2 \) and \( E((n/2) - k) \leq \log_2(k - 2) \). Thus, the bound for \( N(k) \) given in Theorem 6 can be estimated by Lemma 3 as follows: \( N(k) < \frac{1}{4}(k + \log_2 k - 4 + u) \), which, by conditions of the theorem, does not exceed \( k \).

2. \( 2^n ((n/2) - 1) \). Since \( GCD((n/2) - 1, (n/2) - k) \leq k - 1 \) we have that \( E((n/2) - k) \leq \log_2(k - 1) \). Let \( (n/2) - 1 = (2l + 1) 2^n \) for some \( l \) and \( u \); then

\[
A = \left[ (2l + 1) 2^n - \frac{k - 3}{2}, (2l + 1) 2^n - 1 \right].
\]

So, if \( b = (2l + 1) 2^n - i \in A \), then \( E(b) = E(i) \). Therefore,

\[
E \left( \frac{(n/2 - 2)!}{((n - k - 1)/2)!} \right) = E \left( \frac{(k - 3)!}{2} \right) < \frac{k - 5}{2}.
\]

As in the previous subcase we get \( N(k) < \frac{1}{4}(5k + 3 \log_2 k - 7 + 2u) \), which, by conditions of the theorem, does not exceed \( k \).

3. \( 2^n | ((n/2) - k) \). This case is treated similarly, and we get \( N(k) < \frac{1}{4}(5k + 7 \log_2 k - 7 + 3u) \), and again we are through.

Note that the restrictions on \( k \) in the statement of the theorem are of no importance since for small \( k \) existence of noninteger roots can be checked directly.

We would like to mention other possible approaches to a proof of Conjecture 2. They are based on an observation that if all the roots of \( P\alpha(x) \) are integral, then by \((10)\), \( f\alpha(x) = P_{\alpha - k}(x)/P\alpha(x) \) might be a polynomial of degree \( n - 2k \). Considering the expansion \( f\alpha(x) = \sum_{\alpha = 0}^{n - 2k} \gamma\alpha P\alpha(x) \) and, thus, \( P_{\alpha - k}(x) = P\alpha(x) \sum_{\alpha = 0}^{n - 2k} \gamma\alpha P\alpha(x) \). Employing \((13)\) one gets a system of linear equations in \( \gamma\alpha \)'s which seems to be incompatible, but we were unable to prove it. On the other hand, notice that \( f\alpha(x) \), by assumption a polynomial of degree \( n - 2k \), takes alternatively on \( \pm 1 \) in all \( n + 1 - k \) integer points of the interval \( [0, n] \) which are not the roots of \( P\alpha(x) \). This also seems to be quite restrictive.

6. WHEN DO INTEGRAL ROOTS NOT EXIST AT ALL?

In many applications nonexistence of integral roots is of essential importance \([14, 39]\). In view of Theorems 2-4 the most interesting case of the
problem arises when $k$ (or $t$) grows with $n$. Then the diophantine equations become nonpolynomial, and few is known about their solutions. On the other hand the generating function (1) of Krawtchouk polynomials resembles that of binomial coefficient. This suggests that some consideration in the style of the famous Lucas theorem [30] can be useful. As far as we know L. Chihara and D. Stanton were the first to notice it [9]. In this section we try to push it further along this line.

Let us recall the Lucas theorem. Digits of $p$-adic expansion of a number $a = \sum_i a_i(i) p^i$ will be denoted by $a_i(i)$. If $a_i(i) \geq b_j(i)$ for all $i$ then we will write it as $a \geq_p b$.

**Theorem 15** [30, 15]. For $p$ prime

$$\binom{a}{b} \equiv \prod_i \binom{a_i(i)}{b_i(i)} \pmod{p}. \quad (38)$$

In particular,

$$\binom{a}{b} \not\equiv 0 \pmod{2} \quad \text{iff} \quad a \geq_2 b. \quad (39)$$

**Theorem 16.** $N(k) = 0$ if $n \geq_2 k$.

**Proof.** $(1-z)^k (1+z)^{n-k} \equiv (1+z)^n \pmod{2}$, and the result follows from (39).

Now we pass to moduli being powers of 2. The following theorem is a slightly more general version of Theorem 4.3 from [9].

**Theorem 17.** Let $n \geq k + 2^m$. Then $P_k(x) \equiv P_k(x + 2^m) \pmod{2^{m+1}}$.

**Proof.** Using an easy identity $(1+z)^{2^m} \equiv (1-z)^{2^m} \pmod{2^{m+1}}$, we have

\[
(1-z)^k (1+z)^{n-k} - (1-z)^k (1+z)^{2^m} (1+z)^{n-k-2^m} = (1-z)^k (1+z)^{n-k-2^m} (1+z)^{2^m} - (1-z)^{2^m} \equiv 0 \pmod{2^{m+1}} \]

**Corollary 4.** Let $n \geq k + 2^m$ and let $P_k(i) \not\equiv 0 \pmod{2^{m+1}}$ for $i = 0, \ldots, 2^m - 1$, then $P_k(x) \not\equiv 0 \pmod{2^{m+1}}$, and, therefore, $N(k) = 0$.

For instance, if the modulus equals 4 one has to check values of $P_k(0) = \binom{n}{k}$ and $P_k(1) = \binom{(n-2k)}{k}$ modulo 4. For powers of primes there exists a generalization of the Lucas theorem [13]. So one can check in principle the condition on $P_k(0)$. What about $P_k(1)$?
Already modulo 3 the situation is much more complicated, and we give only sufficient conditions for \( P_n^k(x) \equiv 0 \pmod{3} \).

We will use the following identities for Krawtchouk polynomials modulo a prime \( p \).

**Lemma 4.** For any integer \( s \geq 0 \) and \( q = p^r \), \( p \) is a prime,

\[
P_n^k(x) \equiv P_n^{k-q}(x) + P_n^{k+q}(x) \pmod{p};
\]

\[
P_n^k(x) \equiv P_n^{k}(x-q) - P_n^{k-q}(x-q) \pmod{p};
\]

\[
P_n^k(x) \equiv -P_n^{k}(x-q) + 2P_n^{k-q}(x-q) \pmod{p};
\]

and, for \( p = 3 \), \( q = 3^r \),

\[
P_n^k(3)(x-q) + P_n^{k+q}(x-2q) \pmod{3}.
\]

**Proof.** We prove (40). The other identities are derived using the same arguments. The following series of identities is valid

\[
\sum_{k=0}^{\infty} (P_n^k(x) - P_n^{k-q}(x)) z^k
\]

\[
= (1-z)^x (1+z)^{r-x} - (1-z)^x (1+z)^{r-x-q}
\]

\[
= (1-z)^x (1+z)^{r-x-q} ((1+z)^r - 1) \equiv (1-z)^x (1+z)^{r-x-q} z^q
\]

\[
= z^q \sum_{k=0}^{\infty} P_n^{k-q}(x) z^k
\]

\[
= \sum_{k=0}^{\infty} P_n^{k-q}(x) z^k \pmod{p}.
\]

Hence the generating function for \( P_n^k(x) - P_n^{k-q}(x) - P_n^{k+q}(x) \) is identically zero modulo \( p \).

Now we are in a position to prove

**Theorem 18.** Let \( k = k_s 3^s + \cdots + k_0 \), and \( n = n_t 3^t + \cdots + n_0 \), \( n \geq k \),

and \( k_i, n_i \in \{0, 2\}, i = 0, \ldots, s \). Then \( P_n^k(x) \equiv 0 \pmod{3} \) for all integer \( x \), \( 0 \leq x \leq n \).

**Proof.** The proof is by induction on \( n \). Notice that for small \( n \leq 8 \) the claim is easily checked. We will consider several cases.

1. \( n_1 = 2 \). Assume by (9) that \( x < n/2 \). If necessary, replacing \( k \) by \( n-k \) (see (10)) we can suppose that \( s = 1 \) and \( k_1 = 2 \). Choose \( q = 3^1 \). Then by (40): \( P_n^k(x) \equiv P_n^{k+q}(x) + P_n^{k+q}(x) \pmod{3} \).
Since $k > n - q$ and $x \leq n - q$, the first summand at the RHS is zero, according to (1). The second term, after replacing $k - q$ by $n - k$, satisfies the conditions of the theorem since $n - q \geq n/2 \geq x$, and the claim follows from the induction hypothesis.

2. $n_i = 1$, $k_i = k_{i-1} = 0$. Choosing $q = 3^{i-1}$, and assuming $x \leq n/2$, analogously to the previous case we get $P^{n_i}_n(x) \equiv P^{n_i - q}_n(x) \pmod{3}$, which proves the claim, by the induction hypothesis.

3. $n_i = 1$, $n_{i-1} = 2$, $k_i = 0$, $k_{i-1} = 2$.
   (a) $x_i = 1$. Then we use (41), $q = 3^i$, and the proof is as above, because the induction hypothesis can be applied for since $x_i = 1$ we have that $0 \leq x - q \leq n - q$;
   (b) $x_i = 0$, $x_{i-1} = 1$. Then we use (40), $q = 3^i$, and the proof is as above;
   (c) $x_i = 0$, $x_{i-1} = 2$. Choose $q = 3^{i-1}$. By (43) we get: $P^{n_i}_n(x) \equiv P^{n_i - q}_n(x - 2q) + P^{n_i - q}_n(x - 2q) \pmod{3}$. We claim that the first summand vanishes. To demonstrate this apply recursively (42) to it till the argument of the polynomial becomes 0. Observe that final sum is of the form $\sum x_i P^{n_i - q}_n(0)$, where $x_i$ and $\beta_i$ are all integers, and $x \gg \beta$. However, $n - q - \beta$ does not majorize $k$. Hence, by Theorem 15, it equals 0, and the sum vanishes, and induction holds, since $0 \leq x - 2q \leq n - 2q$. Thus all the possibilities are exhausted and the proof is complete.

For arbitrary $p$ prime we have got the following

**Theorem 19.** Let $n, p^i + \cdots + n_0, k = k_0, p^i + \cdots + k_0, x = x_0 p^i + \cdots + x_0$, and $n_i \geq x_i$ for $i = 0, \ldots, s$. Then

$$P^{n}_n(x) \equiv \prod_{i=0}^s P^{n_i}_n(x_i) \pmod{p}. \quad (44)$$

**Proof.** Put $m_i = n_i - x_i$. The following series of congruences hold due to (1):

$$\sum_{s=0}^{n} P^s_n(x) z^s = (1 - z)^x (1 + z)^{x - \delta} = (1 - z)^{x_0} (1 + z)^{x_0} (1 - z)^{x_0} (1 + z)^{x_0} \equiv (1 - z)^{x_0} (1 + z)^{x_0} \equiv (1 - z)^{x_0} (1 + z)^{x_0} \equiv (1 - z)^{x_0} (1 + z)^{x_0} \equiv (1 - z)^{x_0} (1 + z)^{x_0} \equiv \left( \prod_{i=0}^s \sum_{j=0}^{n_i} P^j_n(x_j) z^{j}\right) \prod_{i=0}^s \sum_{j=0}^{n_i} P^j_n(x_j) z^{j} \pmod{p};$$
Comparing the coefficients at $z^k$, and taking into account that $P_0^n(x) = 1$, we obtain the result.

This theorem easily permits tackling the case $n \equiv -1 \pmod{p^{r+1}}$, since the majorization in the claim evidently holds for all $0 \leq x \leq n$. For such $n$, $k$ must consist from those digits for which $P_{k_i}^{n-1}(x) \equiv 0 \pmod{p}$. Evidently, the digits 0 and $p-1$ can be always taken, 2 and $p-3$ are suitable for $p \equiv 3 \pmod{4}$, since $-1$ is a nonsquare for such $p$. Here is the list (for $p < 100$ of all even $k_i \in 0, \ldots, (p-1)/2$)

Further investigations of the values of Krawtchouk polynomials modulo primes seem to be promising. Let us state some conjectures:

**Conjecture 5.** The conditions of Theorem 18 are actually necessary and sufficient for $P_{k_i}^n(x) \equiv 0 \pmod{3}$ for all integral $x$.

Define $H_k(y) = k! P_k((n-y)/2)$.

**Conjecture 6.**

$$H_{k+a}(y) \equiv (H_k(y))^a H_a(y) \pmod{a}.$$

In connection with the last conjecture, notice that for $p$ being a prime we have $H_p(y) = p! Q_p(y) \equiv 0 \pmod{p}$ for all $y \equiv n \pmod{2}$. This follows from the fact that $Q_p(y)$ takes on integer values for such $y$'s. Since the degree of $H_p(y)$ is exactly $p$ then $H_p(y) \equiv y^p - y \pmod{p}$.

**Acknowledgment**

We are grateful to Laurent Habsieger for helpful comments. We also received from him a proof of Conjecture 6. We are also indebted to the anonymous referee for his numerous and valuable suggestions which led to improvement of the paper.
References

18. Y. Hong, On the nonexistence of nontrivial perfect $e$-codes and tight $2e$-designs in Hamming Schemes $H(N, q)$ with $e \geq 3$ and $q \geq 3$, Graphs and Combin. 2 (1986), 145–164.
38. C. L. Siegel, The integer solution of the equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. 1 (1920), 66–68.
45. V. Zinoviev and V. Leontiev, The nonexistence of perfect codes over Galois fields, Problemy upravleniya i teorii informatiki 2 (1973), 123–132. [in Russian]