stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZN 82/78 JULI
(DEPARTMENT OF PURE MATHEMATICS)

M.R. BEST

ON THE EXISTENCE OF PERFECT CODES

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O).

AMS(MOS) subject classification scheme (1970): 05B40, 94A10

On the existence of perfect codes

by

M.R. Best

ABSTRACT

It is proved that only finitely many unknown perfect codes over arbitrary alphabets correcting at least three errors exist.

KEYWORDS & PHRASES: *perfect codes, packing*

0. INTRODUCTION

In this note we prove that only finitely many unknown perfect codes over arbitrary alphabets correcting at least three errors exist. This is an extension of the result of E. BANNAI which states that for each *fixed* $t \geq 3$ only finitely many t-perfect codes exist.

The proof does not make use of the sphere packing condition, but it heavily depends on the generalized Lloyd theorem relating the existence of perfect codes to the zeros of Kravčuk polynomials (lemma 9.2). We list a number of properties of these polynomials in section 2. In particular we make use of the difference equation (lemma 2.4). This equation, together with two elementary results on recurrence relations (section 1), will lead to the conclusion that the distances between consecutive zeros of a Kravčuk polynomial of sufficiently large degree cannot be integral simultaneously. This implies the non-existence of perfect codes correcting sufficiently many errors. Combination with Bannai's theorem yields the theorem stated above.

This note is only a preliminary one. Shorthly a paper will appear in which the bounds are to be made explicit.

1. THREE TERM RECURRENCE RELATIONS

In this section we derive estimates for the solution of a recurrence relation of the type

$$F(x+1) - A(x)F(x) + R(x)F(x-1) = 0$$

in which R does not vanish anywhere.

Without loss of generality we may assume $R = 1$ because of the following substitution. Let g be a function which does not have any zeros and which satisfies the simple two term recursion

$$g(x+1) = R(x)g(x-1),$$

and define G by $F = gG$. Then

$$g(x+1)G(x+1) - A(x)g(x)G(x) + R(x)g(x-1)G(x-1) = 0,$$

so

$$G(x+1) - \frac{A(x)g(x)}{g(x+1)} G(x) + G(x-1) = 0.$$

Defining B by

$$B(x) = \frac{A(x)g(x)}{g(x+1)},$$

we find

$$G(x+1) - B(x)G(x) + G(x-1) = 0.$$

In the next two lemmas we analyze the effect of a perturbation of the function B. In view of later applications we do not restrict ourselves to $x \in \mathbb{Z}$ (which is obviously allowed), but let x run through some subset of $\mathbb{Z}+a$ for some $a \in \mathbb{R}$. The lemmas regain their natural form by taking $a = 1$.

Before stating the lemma, we introduce a notation which will be used throughout this paper. Let a, b be real numbers. Then $[a,b)_{\mathbb{Z}}$, $[a,b]_{\mathbb{Z}}$, $(a,b)_{\mathbb{Z}}$, $(a,b]_{\mathbb{Z}}$ denote the usual intervals $[a,b)$, etc. of the reals, intersected by the set $\mathbb{Z}+a$. So e.g.

$$[a,b)_{\mathbb{Z}} = [a,b) \cap (\mathbb{Z}+a).$$

<u>LEMMA 1.1</u>. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z}+a$, *and* F, G, A *and* B *be real function so that*

$$F(a-1) = G(a-1),$$

$$F(a) = G(a),$$

$$F(k+1) - A(k)F(k) + F(k-1) = 0 \quad \textit{for } k \in [a,b)_{\mathbb{Z}},$$

$$G(k+1) - B(k)G(k) + G(k-1) = 0 \quad \textit{for } k \in [a,b)_{\mathbb{Z}},$$

and

$$F(k) \neq 0 \quad \textit{for } k \in [a,b]_{\mathbb{Z}}.$$

Then

$$F(k)G(k-1) - F(k-1)G(k) = \beta(k) \quad \textit{for } k \in [a,b]_{\mathbb{Z}},$$

and

$$G(k) = (1-\gamma(k))F(k) \quad \textit{for } k \in [a,b]_{\mathbb{Z}},$$

where

$$\gamma(k) = \sum_{i\in(a,k]_{\mathbb{Z}}} \frac{\beta(i)}{F(i)F(i-1)} \quad \textit{for } k \in [a,b]_{\mathbb{Z}},$$

$$\beta(k) = \sum_{i\in[a,k)_{\mathbb{Z}}} \alpha(i) \quad \textit{for } k \in [a,b]_{\mathbb{Z}},$$

and

$$\alpha(k) = (A(k)-B(k))F(k)G(k) \qquad \textit{for } k \in [a,b)_{\mathbb{Z}}.$$

PROOF. For k = a the assertions are clear. Assume that they have been proved for certain $k \in [a,b)_{\mathbb{Z}}$. Then by the two recurrence relations:

$$F(k+1)G(k) - F(k)G(k+1) =$$

$$= (A(k)-B(k))F(k)G(k) + F(k)G(k-1) - F(k-1)G(k) =$$

$$= \alpha(k) + \beta(k) = \beta(k+1),$$

so

$$G(k+1) = \frac{F(k+1)G(k)-\beta(k+1)}{F(k)} =$$

$$= (1-\gamma(k) - \frac{\beta(k+1)}{F(k)F(k+1)})F(k+1) = (1-\gamma(k+1))F(k+1). \quad \square$$

LEMMA 2. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z}+a$, *and* F, G, A *and* B *be real functions so that*

$$F(a-1) = G(a-1) \geq 0$$

$$F(a) \geq G(a),$$

$$A(a) > B(a),$$

$$A(k) \geq B(k) \qquad \textit{for } k \in (a,b)_{\mathbb{Z}},$$

$$F(k+1) - A(k)F(k) + F(k-1) = 0 \qquad \textit{for } k \in [a,b)_{\mathbb{Z}},$$

$$G(k+1) - B(k)G(k) + G(k-1) = 0 \qquad \textit{for } k \in [a,b)_{\mathbb{Z}},$$

$$G(k) > 0 \qquad \textit{for } k \in [a,b)_{\mathbb{Z}},$$

$$G(b) \geq 0.$$

Then

$$F(k)G(k-1) > F(k-1)G(k) \qquad \textit{for } k \in (a,b]_{\mathbb{Z}},$$

and

$$F(k) > G(k) \qquad \textit{for } k \in (a,b]_{\mathbb{Z}}.$$

PROOF. For k = a+1 we have, assuming $b \geq a+1$:

$$F(a+1)G(a) - F(a)G(a+1) =$$

$$= (A(a)-B(a))F(a)G(a) + F(a)G(a-1) - F(a-1)G(a) > 0$$

because of

$$A(a) - B(a) > 0,$$

$$F(a) \geq G(a) > 0.$$

and

$$F(a)G(a-1) - F(a-1)G(a) = F(a)(F(a)-G(a)) \geq 0.$$

Hence

$$F(a+1)G(a) > F(a)G(a+1) \geq G(a)G(a+1),$$

so

$$F(a+1) > G(a+1).$$

Now suppose that the assertions have been proved for certain $k \in (a,b)_{\mathbb{Z}}$. Then

$$F(k+1)G(k) - F(k)G(k+1) =$$

$$= (A(k)-B(k))F(k)G(k) + F(k)G(k-1) - F(k-1)G(k) > 0,$$

because of

$$A(k) - B(k) \geq 0,$$

$$F(k) > G(k) \geq 0 \qquad \text{(induction hypothesis)},$$

and

$$F(k)G(k-1) > F(k-1)G(k) \qquad \text{(induction hypothesis)}.$$

Hence

$$F(k+1)G(k) > F(k)G(k+1) \geq G(k)G(k+1),$$

so

$$F(k+1) > G(k+1).$$

This proves the lemma by induction. □

2. KRAVČUK POLYNOMIALS

Up to section 9, *we assume that* $q > 1$ *and* $n \in \mathbb{N}$.*)

For any $k \in \mathbb{N}$, the Kravčuk polynomial K_k of degree k is defined by

$$K_k(v) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{v}{j} \binom{n-v}{k-j} \quad \text{for all } v \in \mathbb{R}.$$

*) In this note, 0 is considered to belong to $\mathbb{N}$.

A simple expression for the generating formal power series exists.

LEMMA 1. *Let* $v \in \mathbb{R}$. *Then*

$$\sum_{k=0}^{\infty} K_k(v)x^k = (1+(q-1)x)^{n-v}(1-x)^v.$$

PROOF. This follows by taking the Cauchy product of the formal power series expansions of the factors on the right hand side. □

Amongst Kravčuk polynomials the following recurrence relation holds.

LEMMA 2. *Let* $v \in \mathbb{R}$. *Then*

$$(k+1)K_{k+1}(v) - (k+(q-1)(n-k)-qv)K_k(v) + (q-1)(n-k+1)K_{k-1}(v) = 0$$

for each $k \in \mathbb{N}\backslash\{0\}$, *and* $K_0(v) = 1$ *and* $K_1(v) = (q-1)n-qv$.

PROOF. Define $\Phi = \sum_{k=0}^{\infty} K_k(v)x^k$. Then, by lemma 1, Φ satisfies the following differential equation:

$$(1-x)(1+(q-1)x)\frac{\partial\Phi}{\partial x} = ((q-1)(n-v)(1-x)-v(1+(q-1)x))\Phi.$$

Hence

$$(1+(q-2)x-(q-1)x^2)\sum_{k=0}^{\infty} k\ K_k(v)x^{k-1} =$$

$$= ((q-1)n-qv-(q-1)nx)\sum_{k=0}^{\infty} K_k(v)x^k.$$

Comparison of coefficients yields the required relation. □

A certain symmetry between k and v in $K_k(v)$ exists.

LEMMA 3. *Let* $k \in \mathbb{N}$, $v \in \mathbb{N}$. *Then*

$$\binom{n}{v}K_k(v)(q-1)^v = \binom{n}{k}K_v(k)(q-1)^k.$$

PROOF. By lemma 1 we have:

$$\sum_{v=0}^{\infty}\sum_{k=0}^{\infty}\binom{n}{v}K_k(v)(q-1)^v x^k y^v =$$

$$= \sum_{v=0}^{\infty}\binom{n}{v}(1+(q-1)x)^{n-v}(1-x)^v(q-1)^v y^v =$$

$$= (1+(q-1)(x+y-xy))^n.$$

This is symmetric in x and y, hence $\binom{n}{v}K_k(v)(q-1)^v$ is symmetric in k and v. □

From this symmetry relation we derive the following difference equation for Kravčuk polynomials.

LEMMA 4. *Let* $k \in [0,n]_{\mathbb{Z}}$, $v \in \mathbb{R}$. *Then*

$$(q-1)(n-v)K_k(v+1) - (v+(q-1)(n-v)-qk)K_k(v) + vK_k(v-1) = 0.$$

PROOF. According to lemma 2 we have for $v \in \mathbb{N}$ (define $K_{-1} = 0$):

$$(v+1)K_{v+1}(k) - (v+(q-1)(n-v)-qk)K_v(k) + (q-1)(n-v+1)K_{v-1}(k) = 0,$$

so by lemma 3 (after multiplication by $\binom{n}{k}(q-1)^k$):

$$(v+1)\binom{n}{v+1}(q-1)^{v+1}K_k(v+1) - (v+(q-1)(n-v)-qk)\binom{n}{v}(q-1)^vK_k(v) +$$

$$+ (q-1)(n-v+1)\binom{n}{v-1}(q-1)^{v-1}K_k(v-1) = 0.$$

Division by $\binom{n}{v}(q-1)^v$ yields the required relation for $v \in [0,n]_{\mathbb{Z}}$.

Since both sides of the identity are polynomials in v of degree at most n, the identity holds for all $v \in \mathbb{R}$. □

A combined difference recurrence relation also exists.

LEMMA 5. *Let* $k \in \mathbb{N} \setminus \{0\}$, $v \in \mathbb{R}$. *Then*

$$K_k(v+1) - K_k(v) + K_{k-1}(v) + (q-1)K_{k-1}(v+1) = 0.$$

PROOF. From lemma 1 we derive (define $K_{-1} = 0$):

$$\sum_{k=0}^{\infty} (K_k(v+1) - K_k(v) + K_{k-1}(v) + (q-1)K_{k-1}(v+1))x^k =$$

$$= (1+(q-1)x)^{n-v-1}(1-x)^{v+1} - (1+(q-1)x)^{n-v}(1-x)^v +$$

$$+ x(1+(q-1)x)^{n-v}(1-x)^v + (q-1)x(1+(q-1)x)^{n-v-1}(1-x)^{v+1} =$$

$$= (1+(q-1)x)^{n-v-1}(1-x)^v \cdot$$

$$\cdot (1-x - (1+(q-1)x) + x(1+(q-1)x) + (q-1)x(1-x)) = 0. \quad \square$$

We give an alternative presentation of the Kravčuk polynomials.

LEMMA 6. *Let* $k \in \mathbb{N}$. *Then*

$$K_k(v) = \sum_{j=0}^{k} (-1)^j q^{k-j} \binom{n-v}{k-j} \binom{n-k+j}{j} = \frac{q^k}{k!} F(n-v)$$

for all $v \in \mathbb{R}$, *where* F *is defined by*

$$F(w) = \sum_{j=0}^{k} c_j \, w(w-1)(w-2)\dots(w-j+1)$$

for all w, *where*

$$c_j = \left(\frac{-1}{q}\right)^{k-j} \frac{(n-j)!}{(n-k)!} \binom{k}{j} \qquad \textit{for all } j \in [0,k]_{\mathbb{Z}}.$$

Particularly $c_k = 1$, *so* F *is a monic polynomial of degree* k.

PROOF. According to lemma 1, we have

$$\sum_{k=0}^{\infty} K_k(v)x^k = (1-x)^v(1-x+qx)^{n-v} = \sum_{i=0}^{\infty} \binom{n-v}{i}(1-x)^{n-i}(qx)^i =$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \binom{n-v}{i}\binom{n-i}{j}(-x)^j(qx)^i =$$

$$= \sum_{k=0}^{\infty} x^k \sum_{j=0}^{\infty} (-1)^j q^{k-j} \binom{n-v}{k-j}\binom{n-k+j}{j}.$$

This proves the first identity. The others follow straightforwardly. □

In lemma 6 we proved that K_k is indeed a polynomial of degree k. The family $\{K_k \mid k \in \mathbb{N}\}$ is orthogonal on the integers with respect to the weight function ρ defined by $\rho(v) = q^{-n}\binom{n}{v}(q-1)^v$.

LEMMA 7. *Let* $k \in \mathbb{N}$ *and* $\ell \in \mathbb{N}$. *Then*

$$\sum_{v=0}^{n} K_k(v)K_\ell(v)\rho(v) = \delta_{k\ell}\binom{n}{k}(q-1)^k.$$

PROOF.

$$\sum_{k=0}^{\infty} \sum_{\ell=0}^{\infty} \sum_{v=0}^{n} K_k(v)K_\ell(v)\rho(v)x^k y^\ell =$$

$$= \sum_{v=0}^{n} q^{-n}\binom{n}{v}(q-1)^v(1+(q-1)x)^{n-v}(1-x)^v(1+(q-1)y)^{n-v}(1-y)^v =$$

$$= q^{-n}((q-1)(1-x)(1-y) + (1+(q-1)x)(1+(q-1)y))^n =$$

$$= (1+(q-1)xy)^n = \sum_{k=0}^{n} \binom{n}{k}(q-1)^k x^k y^k.$$

Comparison of corresponding coefficients yields the desired orthogonality relation. □

Lemma 7 places the theory of orthogonal polynomials at our disposal. For example, we know that the zeros of K_k are real and simple (cf. SZEGÖ [6], theorem 3.3.1).

3. THE MIDDLEMOST ZERO OF A KRAVČUK POLYNOMIAL

Up to section 9, *we assume that* $q \in \mathbb{N}$, $q > 2$.

In this section we look for zeros of K_k close to $\frac{q-1}{q}n$. E. BANNAI (cf. [1]) proved that for fixed odd k and $n/q \to \infty$ the middlemost zero of K_k asymptotically equals

$$\frac{q-1}{q}n - \frac{(q-2)(k-1)}{3q} + o(1)$$

(cf. proposition 15). We shall not use this result, but show instead that for each odd $k > 1$, a zero occurs in the interval

$$\left(\frac{q-1}{q}n - \frac{(q-2)(k-1)}{q}, \frac{q-1}{n}n\right).$$

For each $v \in \mathbb{R}$, we define y by

$$v = \frac{q-1}{q}n - \frac{q-2}{q}y.$$

For each $k \in \mathbb{N}$, we define the function L_k by

$$L_k(y) = (-1)^{\frac{1}{2}k(k-1)} K_k(v) \quad \text{for all } v \in \mathbb{R}.$$

The recurrence relation from lemma 2.2 can be translated into

<u>LEMMA 1</u>. *Let* $y \in \mathbb{R}$. *Then*

$$(k+1)L_{k+1}(y) = (-1)^{k+1}(q-2)(k-y)L_k(y) + (q-1)(n-k+1)L_{k-1}(y)$$

for all $k \in \mathbb{N}\backslash\{0\}$, *and* $L_0(y) = 1$ *and* $L_1(y) = (q-2)y$.

PROOF.

$$(k+1)(-1)^{\frac{1}{2}k(k+1)}L_{k+1}(y) + (q-2)(k-y)(-1)^{\frac{1}{2}k(k-1)}L_k(y) +$$
$$+ (q-1)(n-k+1)(-1)^{\frac{1}{2}(k-1)(k-2)}L_{k-1}(y) = 0. \quad \square$$

LEMMA 2. *Let* m *be the smallest value of* $k \in \mathbb{N}$ *for which either* $k = n$ *or* L_k *contains at least two zeros in the interval* $(0,k)$. *Then sequences* $(\eta_\ell)_{\ell=0}^{\lfloor\frac{1}{2}m-1\rfloor}$ *and* $(\xi_\ell)_{\ell=1}^{\lfloor\frac{1}{2}(m-1)\rfloor}$ *exist so that* $\eta_0 = 0$ *and so that for each* $\ell \in \mathbb{N}\backslash\{0\}$ *with* $2\ell+1 \le m$ *the following assertions hold*

1. $\eta_{\ell-1} \ge 0$.
2. $L_{2\ell}(\eta_{\ell-1}) > 0$.
3. $L_{2\ell}$ *has at most one zero in* $(\eta_{\ell-1},2\ell)$. *This is* ξ_ℓ *if it exists; otherwise* $\xi_\ell = 2\ell$.
4. $\eta_{\ell-1} < \xi_\ell \le 2\ell$.
5. $L_{2\ell+1}(\xi_\ell) > 0$.
6. $L_{2\ell+1}(\eta_{\ell-1}) < 0$.
7. $L_{2\ell+1}$ *has at least one zero in* $(\eta_{\ell-1},\xi_\ell)$. *If* $2\ell+1 < m$, *then this zero is unique, and equals* η_ℓ.

PROOF. We first prove 1-7 for $\ell = 1$ provided $m \ge 3$.

1. $0 \ge 0$.
2. $L_2(0) > 0$, for $2L_2(0) = (q-2)L_1(0)+(q-1)nL_0(0) = (q-1)\, n > 0$.
3. L_2 has at the most one zero in $(0,2)$ because of $m \ge 3$. Call it ξ_1 if it exists; otherwise define $\xi_1 = 2$.
4. $0 < \xi_1 \le 2$ - obvious.
5. $L_3(\xi_1) > 0$, for $3L_3(\xi_1) = -(q-2)(2-\xi_1) + (q-1)(n-1)L_1(\xi_1) > 0$, since $(2-\xi_1)L_2(\xi_1) = 0$ (3), and $L_1(\xi_1) > 0$ because of $\xi_1 > 0$ (4).
6. $L_3(0) < 0$, for $3L_3(0) = -2(q-2)L_2(0) + (q-1)(n-1)L_1(0) < 0$, since $L_2(0) > 0$ (2) and $L_1(0) = 0$.

7. L_3 has at least one zero in $(0,\xi_1)$. This follows from 4, 5 and 6. If $m > 3$, this zero is unique because of $\xi_1 < 3$ (4). Call it η_1.

Now suppose that $\ell \geq 2$, $m \geq 2\ell+1$, and that 1-7 have been proved for $\ell-1$ instead of ℓ. We prove 1-7:

1. Follows from $\eta_{\ell-1} > \eta_{\ell-2} \geq 0$ (7, 1).

2.*) Assume that $L_{2\ell-2}(\eta_{\ell-1}) \leq 0$. Since $L_{2\ell-2}(\eta_{\ell-2}) > 0$ (2) and $\eta_{\ell-2} < \eta_{\ell-1}$ (7), $L_{2\ell-2}$ has a zero in the interval $(\eta_{\ell-2},\eta_{\ell-1}]$. Since $\eta_{\ell-2} \leq 2\ell-2$ (4), $L_{2\ell-2}$ has a zero in the interval $(\eta_{\ell-2},2\ell-2]$. According to 3 this zero is unique, so it equals $\xi_{\ell-1}$. From 7 follows that $\xi_{\ell-1} > \eta_{\ell-1}$, so $\xi_{\ell-1} \notin (\eta_{\ell-2},\eta_{\ell-1}]$. Contradiction. Hence $L_{2\ell-2}(\eta_{\ell-1}) > 0$. Since $L_{2\ell-1}(\eta_{\ell-1}) = 0$ (7), and $n-2\ell+2 \geq n-m+3 \geq 3$, we find

$$2\ell L_{2\ell}(\eta_{\ell-1}) = (q-2)(2\ell-1-\eta_{\ell-1})L_{2\ell-1}(\eta_{\ell-1}) + (q-1)(n-2\ell+2)L_{2\ell-2}(\eta_{\ell-1}) > 0.$$

3. From $\eta_{\ell-1} \geq 0$ (1) follows $(\eta_{\ell-1},2\ell) \subseteq (0,2\ell)$. Since $m \geq 2\ell+1$, $L_{2\ell}$ has at the most one zero in $(\eta_{\ell-1},2\ell)$. Call it ξ_ℓ if it exists; otherwise define $\xi_\ell = 2\ell$.

4. If $\xi_\ell \in (\eta_{\ell-1},2\ell)$, then obvious.
If $\xi_\ell = 2\ell$, then $\eta_{\ell-1} < \xi_{\ell-1} \leq 2\ell-2 < \xi_\ell \leq 2\ell$ (7,4).

5. Suppose that $L_{2\ell-1}(\xi_\ell) \leq 0$. Since $L_{2\ell-1}(\xi_{\ell-1}) > 0$ (5), $\eta_{\ell-1} < \xi_{\ell-1}$ (7) and $\eta_{\ell-1} < \xi_\ell$ (4), $L_{2\ell-1}$ has, beside in $\eta_{\ell-1}$, another zero in the interval $[\xi_\ell,\xi_{\ell-1}) \cup (\xi_{\ell-1},\xi_\ell]$. Since $L_{2\ell}$ does not have zeros in $(\eta_{\ell-1},\xi_\ell)$ (3), we must have $\xi_\ell < \xi_{\ell-1}$ (cf. SZEGÖ [6], thm. 3.3.2). Since $\xi_{\ell-1} < 2\ell-1$ (4), $L_{2\ell-1}$ has two zeros in the interval $(0,2\ell-1)$. Hence $2\ell-1 \geq m$. Contradiction.
Consequently, $L_{2\ell-1}(\xi_\ell) > 0$. Since $(2\ell-\xi_\ell)L_{2\ell}(\xi_\ell) = 0$ and $n-2\ell+1 \geq n-m+2 \geq 2$, we find

$$(2\ell+1)L_{2\ell+1}(\xi_\ell) = -(q-2)(2\ell-\xi_\ell)L_{2\ell}(\xi_\ell) + (q-1)(n-2\ell+1)L_{2\ell-1}(\xi_\ell) > 0.$$

---

*) This claim can also be derived from the facts that the zeros of $L_{2\ell}$ and $L_{2\ell-1}$ are interlaced, and that $L_{2\ell-1}$ vanishes and increases in $\eta_{\ell-1}$.

6. Since $\eta_{\ell-1} < 2\ell$ (4), $L_{2\ell}(\eta_{\ell-1}) > 0$ (2), and $L_{2\ell-1}(\eta_{\ell-1}) = 0$ (7), we find

$$(2\ell+1)L_{2\ell+1}(\eta_{\ell-1}) = -(q-2)(2\ell-\eta_{\ell-1})L_{2\ell}(\eta_{\ell-1}) + (q-1)(\eta-2\ell+1)L_{2\ell-1}(\eta_{\ell-1}) < 0.$$

7. $L_{2\ell+1}$ has at least one zero in $(\eta_{\ell-1},\xi_\ell)$. This follows from 4,5 and 6. If $2\ell+1 < m$, this zero is unique because of $0 \le \eta_{\ell-1} < \xi_\ell < 2\ell+1$ (1,4). Call it η_ℓ. □

LEMMA 3. *Let* k *be an odd integer,* $3 \le k \le n$. *Then* K_k *has a zero* v_0 *with*

$$v_0 \in \left(\frac{q-1}{q}\,n - \frac{q-2}{q}\,(k-1),\ \frac{q-1}{q}\,n\right).$$

PROOF. According to lemma 2 (1,4,7), $L_{2\ell+1}$ has a zero in the interval $(0,2\ell)$ provided $3 \le 2\ell+1 \le m$. Hence if $k \le m$, then L_k has a zero in $(0,k-1)$. Furthermore, L_m has at least two zeros in $(0,m)$ provided $m < n$, so if $m < k \le n$, then L_k has a zero in $(0,m)$, so in $(0,k-1)$ (cf. SZEGÖ [6], thm. 3.3.3). Hence for each odd k with $3 \le k \le n$, L_k has a zero in $(0,k-1)$. The lemma follows from the definition of L_k. □

4. KRAVČUK POLYNOMIALS WITH INTEGRAL ZEROS

Up to section 9, *we assume that* $t \in \mathbb{N}$, $n \ge t$, *and that* K_t *has only integral zeros.*

From this "Lloyd-condition" we shall derive several consequences concerning the possible values of q, n and t, but first we make an almost trivial remark on the position of the zeros of K_t.

LEMMA 1. K_t *does not have zeros in two consecutive integers.*

PROOF. Suppose the contrary. Then the difference equation (lemma 2.4) would imply that K_t has zeros in all integers $0,1,\ldots,n$, which implies $t > n$, contradicting our assumption. □

LEMMA 2. *For each* $j \in [0,t]_{\mathbb{Z}}$,

$$\prod_{i=1}^{j} \frac{(t-i+1)(n-t+i)}{qi} \in \mathbb{Z}.$$

PROOF. According to lemma 2.6 and the notation used there (with $k = t$), F is a monic polynomial with integral zeros, hence with integral coefficients. This implies $c_j \in \mathbb{Z}$ for $j \in [0,t]_{\mathbb{Z}}$. (Proof by induction on j.) Now the lemma follows from

$$(-1)^j c_j = \prod_{i=1}^{j} \frac{(t-i+1)(n-t+i)}{qi} . \quad \square$$

From lemma 2, upper bounds for q and t in terms of n can be derived. Below, we prove some bounds which are sufficient for our purposes. But that does not alter the fact that better estimates are possible.

LEMMA 3. *If* $n \geq 1$, *then* $t < 2 \log n$.

PROOF.*) From lemma 2 with $j = t$ follows

$$\frac{n(n-1). \ \ldots \ .(n-t+1)}{q^t} \in \mathbb{Z}.$$

Let p^α be a prime power dividing q. Then

$$p^{\alpha t} | n(n-1). \ \ldots \ .(n-t+1),$$

so

$$p^{\alpha t-(\lfloor t/p \rfloor + \lfloor t/p^2 \rfloor + \ldots)} | \ n-\tau \quad \text{for some } \tau \in [0,t)_{\mathbb{Z}},$$

so

$$p^{\alpha t - t/(p-1)} \leq n.$$

Hence

$$t(\alpha - \frac{1}{p-1}) \log p \leq \log n.$$

If q is a power of 2, choose $p = 2$, $\alpha = 2$. Then $t \log 2 \leq \log n$.
If q is not a power of 2, choose $p \geq 3$, $\alpha = 1$. Then $\frac{1}{2}t \log 3 \leq \log n$.

In both cases the assertion of the lemma follows. $\square$

LEMMA 4. *If* $t \geq 2$, *then* $q^2 < nt^3$.

---

*) The idea of the proof is due to A. TIETÄVÄINEN (cf. [7]).

PROOF. Lemma 2 yields for $j = 1$:

$$\frac{t(n-t+1)}{q} = \lambda \in \mathbb{Z},$$

and for $j = 2$:

$$\frac{t(n-t+1)}{q} \cdot \frac{(t-1)(n-t+2)}{2q} = \frac{\lambda^2(t-1)(n-t+2)}{2t(n-t+1)} \in \mathbb{Z}.$$

Hence

$$n-t+1 \mid \lambda^2(t-1) = \frac{t^2(t-1)(n-t+1)^2}{q^2},$$

so

$$q^2 \mid t^2(t-1)(n-t+1).$$

From this the lemma follows immediately. □

Up to section 9, we assume that t *is sufficiently large.*

LEMMA 5. $qt^3 \le n$.

PROOF. Immediate from lemma 3 and 4. □

5. THE DIFFERENCE EQUATION OF A KRAVČUK POLYNOMIAL

In lemma 2.4 we proved the following difference equation for K_t:

$$(q-1)(n-v)K_t(v+1) - (v+(q-1)(n-v)-qt)K_t(v) + vK_t(v-1) = 0.$$

We transform this equation according to the method of §1 into a form which allows us to apply the lemmas 1.1 and 1.2. We define the function L by

$$K_t(v) = (q-1)^{-\frac{1}{2}v}(\tfrac{1}{2}v-\tfrac{1}{2})!(\tfrac{1}{2}n-\tfrac{1}{2}v-\tfrac{1}{2})!L(v) \qquad \text{for all } v \in (-1,n+1),$$

where $x! = \Gamma(x+1)$. Then

LEMMA 1.

$$L(v+1) - \frac{v+(q-1)(n-v)-qt}{2\sqrt{q-1}} \cdot \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!} L(v) + L(v-1) = 0$$

for all $v \in (0,n)$.

PROOF. By lemma 2.4 and the definition of L we have

$$2(q-1)^{-\frac{1}{2}v+\frac{1}{2}}(\tfrac{1}{2}v)!(\tfrac{1}{2}n-\tfrac{1}{2}v)!L(v+1) +$$

$$-\ (v+(q-1)(n-v)-qt)(q-1)^{-\frac{1}{2}v}(\tfrac{1}{2}v-\tfrac{1}{2})!(\tfrac{1}{2}n-\tfrac{1}{2}v-\tfrac{1}{2})!L(v) +$$

$$+\ 2(q-1)^{-\frac{1}{2}v+\frac{1}{2}}(\tfrac{1}{2}v)!(\tfrac{1}{2}n-\tfrac{1}{2}v)!L(v-1) = 0.$$

Division by $2(q-1)^{-\frac{1}{2}v+\frac{1}{2}}(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!$ yields the required identity. □

In the following lemmas, the coefficient of $L(v)$ will be estimated.

LEMMA 2.
$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!} = -\tfrac{1}{2}\log(\tfrac{1}{2}v) - \frac{1}{4v} + O(\frac{1}{v^2}) \quad \textit{for } v \to \infty.$$

PROOF. By Stirling's formula we have

$$\log x! = (x+\tfrac{1}{2})\log x - x + \tfrac{1}{2}\log(2\pi) + \frac{1}{12x} + O(\frac{1}{x^2}) \qquad \text{for } x \to \infty,$$

so

$$\log(\tfrac{1}{2}v)! = (\tfrac{1}{2}v+\tfrac{1}{2})\log(\tfrac{1}{2}v) - \tfrac{1}{2}v + \tfrac{1}{2}\log(2\pi) + \frac{1}{6v} + O(\frac{1}{v^2}) \quad \text{for } v \to \infty,$$

and

$$\log(\tfrac{1}{2}v-\tfrac{1}{2})! = \tfrac{1}{2}v\log(\tfrac{1}{2}v-\tfrac{1}{2}) - \tfrac{1}{2}v + \tfrac{1}{2} + \tfrac{1}{2}\log(2\pi) + \frac{1}{6v} + O(\frac{1}{v^2}) \quad \text{for } v \to \infty.$$

Hence

$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!} = -\tfrac{1}{2}\log(\tfrac{1}{2}v) + \tfrac{1}{2}v\log(1-\frac{1}{v}) + \tfrac{1}{2} + O(\frac{1}{v^2}) =$$

$$= -\tfrac{1}{2}\log(\tfrac{1}{2}v) - \tfrac{1}{2}v(\frac{1}{v} + \frac{1}{2v^2}) + \tfrac{1}{2} + O(\frac{1}{v^2}) =$$

$$= -\tfrac{1}{2}\log(\tfrac{1}{2}v) - \frac{1}{4v} + O(\frac{1}{v^2}) \quad \text{for } v \to \infty. \quad \square$$

It turns out that is easier to work with $\frac{q-1}{q}n-v$ instead of v. Therefore we define x by

$$x = \frac{q-1}{q}n - v,$$

and the functions M and a by

$$M(x) = L(v)$$

and

$$a(x) = \frac{v+(q-1)(n-v)-qt}{2\sqrt{q-1}} \cdot \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!} \quad \text{for all } v \in (0,n).$$

The constants implied by the Landau-Bachmann O-symbol and by the Vinogradov <<- and >>- symbols are absolute.

LEMMA 3.

$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!} =$$

$$= -\log\frac{n\sqrt{q-1}}{2q} - \frac{q(q-2)x}{2(q-1)n} - \frac{q^2}{4(q-1)n} + \frac{q^2(q^2-2q+2)x^2}{4(q-1)^2n^2} +$$

$$+ \frac{q^3(q-2)x}{4(q-1)^2n^2} - \frac{q^3(q-2)(q^2-q+1)x^3}{6(q-1)^3n^3} + O(\frac{q^2}{n^2}) \quad \textit{for} \quad |x| \le 9\sqrt{\frac{n}{qt}}\ .$$

PROOF. From the definition of x follows

$$v = \frac{(q-1)n}{q} - x = \frac{(q-1)n}{q}\left(1-\frac{qx}{(q-1)n}\right) \to \infty \quad \text{for } t \to \infty,$$

and

$$n-v = \frac{n}{q} + x = \frac{n}{q}(1+\frac{qx}{n}) \to \infty \qquad \text{for } t \to \infty \text{ (cf. lemma 4.5).}$$

Hence

$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!} =$$

$$= -\tfrac{1}{2}\log(\tfrac{1}{2}v) - \frac{1}{4v} - \tfrac{1}{2}\log(\tfrac{1}{2}(n-v)) - \frac{1}{4(n-v)} + O(\frac{q^2}{n^2}) =$$

$$= -\tfrac{1}{2}\log\left(\frac{(q-1)n}{2q}\left(1-\frac{qx}{(q-1)n}\right)\right) - \frac{q}{4(q-1)n}\left(1-\frac{qx}{(q-1)n}\right)^{-1} +$$

$$-\tfrac{1}{2}\log\left(\frac{n}{2q}\left(1+\frac{qx}{n}\right)\right) - \frac{q}{4n}\left(1+\frac{qx}{n}\right)^{-1} + O(\frac{q^2}{n^2}) =$$

$$= -\tfrac{1}{2}\log\frac{(q-1)n^2}{4q^2} + \frac{qx}{2(q-1)n} + \frac{q^2x^2}{4(q-1)^2n^2} + \frac{q^3x^3}{6(q-1)^3n^3} + O(\frac{x^4}{n^4}) +$$

$$- \frac{q}{4(q-1)n} - \frac{q^2x}{4(q-1)^2n^2} + O(\frac{x^2}{n^3}) - \frac{qx}{2n} + \frac{q^2x^2}{4n^2} - \frac{q^3x^3}{6n^3} + O(\frac{q^4x^4}{n^4}) +$$

$$- \frac{q}{4n} + \frac{q^2x}{4n^2} + O(\frac{q^3x^2}{n^3}) + O(\frac{q^2}{n^2}) =$$

$$= -\log\frac{n\sqrt{q-1}}{2q} - \frac{q(q-2)x}{2(q-1)n} - \frac{q^2}{4(q-1)n} + \frac{q^2(q^2-2q+2)x^2}{4(q-1)^2n^2} +$$

$$+ \frac{q^3(q-2)x}{4(q-1)^2n^2} - \frac{q^3(q-2)(q^2-q+1)x^3}{6(q-1)^3n^3} + O(\frac{q^2}{n^2}). \quad \square$$

LEMMA 4.

$$\log a(x) = \log 2 - \frac{q^2(2t+1)}{4(q-1)n} + \frac{q^4x^2}{8(q-1)^2n^2} + \frac{q^3(q-2)(t+1)x}{4(q-1)^2n^2} +$$

$$- \frac{q^5(q-2)x^3}{8(q-1)^3n^3} - \frac{q^4t^2}{8(q-1)^2n^2} + O(\frac{q^2}{n^2}) \quad \textit{for } |x| \le 9\sqrt{\frac{n}{qt}}.$$

PROOF.

$$\frac{v+(q-1)(n-v)-qt}{2\sqrt{q-1}} = \frac{(q-1)n-qx+(q-1)(n+qx)-q^2t}{2q\sqrt{q-1}} =$$

$$= \frac{2(q-1)n+q(q-2)x-q^2}{2q\sqrt{q-1}} = \frac{n\sqrt{q-1}}{q}\left(1 + \frac{q(q-2)x}{2(q-1)n} - \frac{q^2t}{2(q-1)n}\right),$$

so

$$\log \frac{v+(q-1)(n-v)-qt}{2\sqrt{q-1}} =$$

$$= \log \frac{n\sqrt{q-1}}{q} + \frac{q(q-2)x}{2(q-1)n} - \frac{q^2t}{2(q-1)n} - \frac{q^2(q-2)^2x^2}{8(q-1)^2n^2} + \frac{q^3(q-2)tx}{4(q-1)^2n^2} +$$

$$- \frac{q^4t^2}{8(q-1)^2n^2} + \frac{q^3(q-2)^3x^3}{24(q-1)^3n^3} + O(\frac{q^3x^2t}{n^3}) + O(\frac{q^4x^4}{n^4}).$$

Hence

$$\log a(x) = \log 2 - \frac{q^2(2t+1)}{4(q-1)n} + \frac{q^4x^2}{8(q-1)^2n^2} + \frac{q^3(q-2)(t+1)x}{4(q-1)^2n^2} +$$

$$- \frac{q^5(q-2)x^3}{8(q-1)^3n^3} - \frac{q^4t^2}{8(q-1)^2n^2} + O(\frac{q^2}{n^2}). \qquad \square$$

In order to simplify the formulas, we introduce the variable σ by defining

$$\sigma = \frac{q}{\sqrt{2(q-1)n}}.$$

Then $\sigma \ge \sqrt{\frac{q}{2n}}$ and $\sigma^2t^3 = \frac{q^2t^3}{2(q-1)n} \le \frac{q}{2(q-1)} \le 1$, so $\sigma \le t^{-3/2}$ (cf. lemma 4.5).

Now we can summarize the lemmas 1 and 4 into

LEMMA 5. $M(x+1) - a(x)M(x) + M(x-1) = 0,$

where

$$\log a(x) = \log 2 - \tfrac{1}{2}\sigma^2(2t+1) + \tfrac{1}{2}\sigma^4x^2 + \frac{q-2}{q}\sigma^4(t+1)x +$$

$$- \frac{q-2}{q}\sigma^6x^3 - \tfrac{1}{2}\sigma^4t^2 + O(\sigma^4) \quad \textit{for } |x| \le 9\sqrt{\frac{n}{qt}}\ . \ \Box$$

6. THE FUNCTIONS A AND B

Let x_0 be a real variable in the interval $[-2,t+1]$, which is allowed to depend on q, t and n. This dependence will be specified later. Define y by

$$y = x - x_0$$

and the function A by

$$A(y) = a(x).$$

If $|y| \le \frac{5}{\sigma\sqrt{t}}$, then $|x| \le |y| + |x_0| \le \frac{5}{\sigma\sqrt{t}} + t \le (5\sqrt{2}+1)\sqrt{\frac{n}{qt}} \le 9\sqrt{\frac{n}{qt}}$.

Hence by lemma 5.5:

$$\log A(y) = \log a(x) =$$

$$= \log 2 - \tfrac{1}{2}\sigma^2(2t+1) + \tfrac{1}{2}\sigma^4(y+x_0^2)^2 + \frac{q-2}{q}\sigma^4(t+1)(y+x_0) - \frac{q-2}{q}\sigma^6(y+x_0)^3 +$$

$$- \tfrac{1}{2}\sigma^4t^2 + O(\sigma^4) =$$

$$= \log 2 - \tfrac{1}{2}\sigma^2(2t+1) + \tfrac{1}{2}\sigma^4y^2 + \sigma^4(\frac{q-2}{q}(t+1)+x_0)y +$$

$$- \tfrac{1}{2}\sigma^4(t^2-2\,\frac{q-2}{q}(t+1)x_0-x_0^2) - \frac{q-2}{q}\sigma^6y^3 + O(\sigma^4).$$

First, we derive from this a coarse estimate for A(y):

LEMMA 1. $2\cos(2\sigma\sqrt{t}) < A(y) < 2\cos(\sigma\sqrt{t})$ *for* $|y| \le \frac{5}{\sigma\sqrt{t}}$.

PROOF. This follows from $\sigma\sqrt{t} \to 0$ for $t \to \infty$,

$$\log A(y) = \log 2 - \sigma^2 t + o(\sigma^2 t) \qquad \text{for } t \to \infty,$$

so

$$A(y) = 2(1 - \sigma^2 t + o(\sigma^2 t)) \qquad \text{for } t \to \infty,$$

$$2\cos(2\sigma\sqrt{t}) = 2(1 - 2\sigma^2 t + o(\sigma^2 t)) \qquad \text{for } t \to \infty,$$

$$2\cos(2\sigma\sqrt{t}) = 2(1 - \tfrac{1}{2}\sigma^2 t + o(\sigma^2 t)) \qquad \text{for } t \to \infty. \quad \square$$

Now define the function B by

$$B(y) = A(-y).$$

Then one has for $|y| \le \frac{5}{\sigma\sqrt{t}}$:

$$\log B(y) = \log 2 - \tfrac{1}{2}\sigma^2(2t+1) + \tfrac{1}{2}\sigma^4 y^2 - \sigma^4(\tfrac{q-2}{q}(t+1)+x_0)y + $$
$$- \tfrac{1}{2}\sigma^4(t^2-2\,\tfrac{q-2}{q}(t+1)x_0-x_0^2) + \tfrac{q-2}{q}\,\sigma^6 y^3 + O(\sigma^4),$$

hence

$$\log A(y) - \log B(y) = 2\sigma^4(\tfrac{q-2}{q}(t+1)+x_0)y - 2\,\tfrac{q-2}{q}\,\sigma^6 y^3 + O(\sigma^4).$$

From this upper and lower estimates for $A(y) - B(y)$ will be derived.

<u>LEMMA 2</u>. $A(y) - B(y) \ll \sigma^3\sqrt{t}$ *for* $|y| \le \frac{5}{\sigma\sqrt{t}}$.

<u>PROOF</u>. $\log A(y) - \log B(y) \ll \sigma^4 ty + \sigma^6 y^3 + \sigma^4 \ll \sigma^3\sqrt{t}$,

so

$$A(y) - B(y) = A(y)\left(1 - \frac{B(y)}{A(y)}\right) \ll \left|\log \frac{B(y)}{A(y)}\right| \ll \sigma^3\sqrt{t}. \quad \square$$

<u>LEMMA 3</u>. $A(y) > B(y)$ *for* $\frac{1}{2} \le y \le \frac{5}{\sigma\sqrt{t}}$.

<u>PROOF</u>. $\log A(y) - \log B(y) \gg \sigma^4 ty + O(\sigma^6 y^3) + O(\sigma^4) =$

$$= \sigma^4 ty(1 + O(\frac{\sigma^2 y^2}{t}) + O(\frac{1}{ty})) = \sigma^4 ty(1 + O(\tfrac{1}{t})) \gg \sigma^4 ty > 0. \quad \square$$

7. THE CASE t EVEN

If t is odd, M has a zero very close to the origin, from which we can start the recursion to find the neighbouring zeros. However, in case t is even, then generally no such zeros exist, so we need some extra preparation.

We assume that t is even. We aim to choose an x_0 close to 0 so that $M(x_0-\frac{1}{2}) = M(x_0+\frac{1}{2})$, or, equivalently, a v_0 close to $\frac{q-1}{q}n$ so that $L(v_0-\frac{1}{2}) = L(v_0+\frac{1}{2})$. The corresponding problem for K_t instead of L is fairly easy, but the multiplication factor in the definition of L makes our task cumbersome.

LEMMA 1. *There is a* $v_0 \in (\frac{q-1}{q}n-t, \frac{q-1}{q}n+\frac{3}{2}]$ *so that* $L(v_0-\frac{1}{2}) = L(v_0+\frac{1}{2})$.

PROOF. We introduce the abbreviation $\nu = \frac{q-1}{q}n$. According to lemma 3.3 there is an $\alpha \in (\nu-t+2,\nu)$ so that $K_{t-1}(\alpha) = 0$. From lemma 2.4 one obtains

$$(q-1)(n-\alpha)K_{t-1}(\alpha+1) + \alpha K_{t-1}(\alpha-1) = 0,$$

so $K_{t-1}(\alpha-1)$ and $K_{t-1}(\alpha+1)$ have opposite signs. In order not to be forced to distinguish between two completely similar cases, we introduce the number $\theta \in \{1,-1\}$ as the sign of $K_{t-1}(\alpha+1)$. Then $\theta K_{t-1}(\alpha-1) < 0$ and $\theta K_{t-1}(\alpha+1) > 0$.

K_{t-1} cannot have any zeros in $(\alpha-1,\alpha+1)$ other than α, since otherwise by the interlacing property of the zeros of orthogonal polynomials, K_t would have two (integral) zeros in $(\alpha-1,\alpha+1)$, contradicting lemma 4.1. Hence θK_{t-1} is increasing in α.

Again since the zeros of K_{t-1} and K_t are interlaced, and since $K_{t-1}(0)$ and $K_t(0)$ are both positive, $\theta K_t(\alpha)$ is positive.

By lemma 2.5:

$$K_t(\alpha-1) = K_t(\alpha) + K_{t-1}(\alpha-1) + (q-1)K_{t-1}(\alpha),$$

so

$$\theta K_t(\alpha-1) < \theta K_t(\alpha).$$

We also claim that $\theta K_t(\alpha-2) < \theta K_t(\alpha)$. Suppose on the contrary that $\theta K_t(\alpha-2) \geq \theta K_t(\alpha)$. Since $\theta K_t(\alpha-2) - \theta K_t(\alpha-1) > 0$ and $\theta K_t(\alpha-1) - \theta K_t(\alpha) < 0$, there is a $\beta \in (\alpha-1,\alpha)$ so that $K_t(\beta-1) - K_t(\beta) = 0$. Now

$$K_{t-1}(\beta-1) + (q-1)K_{t-1}(\beta) = K_t(\beta-1) - K_t(\beta) = 0,$$

so $K_{t-1}(\beta-1)$ and $K_{t-1}(\beta)$ have opposite signs, so there is a $\gamma \in [\beta-1,\beta] \subseteq (\alpha-2,\alpha)$ with $K_{t-1}(\gamma) = 0$. Hence K_t must have a zero $\delta \in (\gamma,\alpha) \subseteq (\alpha-2,\alpha)$. But $\theta K_t(\alpha-2)$ and $\theta K_t(\alpha)$ are both positive, so K_t must have yet another (integral) zero in $(\alpha-2,\alpha)$, contradicting lemma 4.1. This proves our claim that $\theta K_t(\alpha-2) < \theta K_t(\alpha)$.

Our next claim is that $\theta L(\alpha-2) < \theta L(\alpha)$. This follows from

$$\theta L(\alpha-2) = \frac{(q-1)^{\frac{1}{2}\alpha-1}}{(\frac{1}{2}\alpha-\frac{3}{2})!(\frac{1}{2}n-\frac{1}{2}\alpha+\frac{1}{2})!}\,\theta K_t(\alpha-2) < \frac{(q-1)^{\frac{1}{2}\alpha-1}}{(\frac{1}{2}\alpha-\frac{3}{2})!(\frac{1}{2}n-\frac{1}{2}\alpha+\frac{1}{2})!}\,\theta K_t(\alpha) =$$

$$= \frac{(q-1)^{\frac{1}{2}\alpha-1}}{(\frac{1}{2}\alpha-\frac{3}{2})!(\frac{1}{2}n-\frac{1}{2}\alpha+\frac{1}{2})!}\cdot\frac{(\frac{1}{2}\alpha-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}\alpha-\frac{1}{2})!}{(q-1)^{\frac{1}{2}\alpha}}\,L(\alpha) =$$

$$= \frac{\alpha-1}{(q-1)(n-\alpha+1)}\,\theta L(\alpha) \le \theta L(\alpha),$$

since $\alpha-1 \le \frac{q-1}{q}n$. From this it follows that there is a $\beta \in \{\alpha-1,\alpha\}$ so that $\theta L(\beta-1) < \theta L(\beta)$.

On the other hand we know that

$$K_t(\alpha) = K_t(\alpha+1) + K_{t-1}(\alpha) + (q-1)K_{t-1}(\alpha+1),$$

so

$$\theta K_t(\alpha) > \theta K_t(\alpha+1).$$

We distinguish between two cases:

i) K_t has a zero in between α and $\nu+2$. Let β be the smallest such zero. Then obviously $L(\beta) = 0$ and $\theta L(\beta-1) \ge 0$, so $\theta L(\beta-1) \ge \theta L(\beta)$.

ii) K_t has no zeros in between α and $\nu+2$. We then claim that $\theta K_t(\nu) \ge \theta K_t(\nu+2)$. Suppose on the contrary that $\theta K_t(\nu) < \theta K_t(\nu+2)$. Then there is a $\beta \in \{\nu,\nu+1\}$ such that $\theta K_t(\beta) > \theta K_t(\beta+1)$. Hence there is a $\gamma \in (\alpha,\beta) \subseteq (\alpha,\nu+1)$ so that $K_t(\gamma) = K_t(\gamma+1)$. Now

$$K_{t-1}(\gamma) + (q-1)K_{t-1}(\gamma+1) = K_t(\gamma) - K_t(\gamma+1) = 0,$$

so there is a $\delta \in [\gamma,\gamma+1] \subseteq (\alpha,\nu+2)$ with $K_{t-1}(\delta) = 0$. Hence K_t must have a zero in between α and δ, contradicting our assumption. This proves our claim that $\theta K_t(\nu) \geq \theta K_t(\nu+2)$.

Now the corresponding inequality for L follows using the same argument as above:

$$\theta L(\nu) \geq \frac{\nu+1}{(q-1)(m-\nu-1)}\, \theta L(\nu+2) \geq \theta L(\nu+2),$$

since $\nu+1 \geq \frac{q-1}{q} n$.

This implies that there is a $\beta \in \{\nu+1,\nu+2\}$ such that $\theta L(\beta-1) \geq \theta L(\beta)$.

Thus we have proved that $\theta L(\beta-1) - \theta L(\beta)$ assumes (weakly) positive as well as negative values on $[\alpha-1,\nu+2]$. So a $\beta \in (\nu-t+\frac{1}{2},\nu+2]$ exists for which $L(\beta-1) = L(\beta)$. This proves the lemma. □

We choose in this section

$$x_0 = \frac{q-1}{q} n - v_0,$$

where v_0 has been defined in lemma 1 above. Then indeed

$$-\frac{3}{2} \leq x_0 < t.$$

Now

$$M(x_0-\tfrac{1}{2}) = M(x_0+\tfrac{1}{2}).$$

In this section we define F by

$$F(y) = \frac{M(x)}{M(x_0+\frac{1}{2})},$$

and y_0 to be the smallest zero of F in the interval $(0, \frac{\pi}{2\sigma\sqrt{t}} + 1)$, provided such zeros exist; otherwise, we define $y_0 = \frac{\pi}{2\sigma\sqrt{t}} + 1$.

Note that the zeros of F are simple and have mutual distance at least 2 (cf. lemma 4.1), and that

$$F(-\tfrac{1}{2}) = F(\tfrac{1}{2}) = 1.$$

Moreover, by the definition of A and lemma 5.5, F satisfies the difference equation

$$F(y+1) - A(y)F(y) + F(y-1) = 0.$$

LEMMA 2. $F(y) \ll \cos(\sigma y\sqrt{t})$ *for* $y \in [\frac{1}{2}, y_0]_{\mathbb{Z}}$,

$$y_0 < \frac{\pi}{2\sigma\sqrt{t}} + 1,$$

and

y_0 *is the smallest positive zero of* F.

PROOF. We first note that $y_0 \le \frac{\pi}{2\sigma\sqrt{t}} + 1 \le \frac{5}{\sigma\sqrt{t}}$.
If $G(y+1) - 2\cos(\sigma\sqrt{t})G(y) + G(y-1) = 0$, $G(-\frac{1}{2}) = G(\frac{1}{2}) = 1$, then

$$G(y) = \frac{\cos(\sigma y\sqrt{t})}{\cos(\frac{1}{2}\sigma\sqrt{t})} \qquad \text{for } y \in \mathbb{Z}+\tfrac{1}{2}.$$

The first assertion of the lemma now follows from lemma 1.2 with $a = \frac{1}{2}$, $b = \lfloor y_0 - \frac{1}{2} \rfloor + \frac{1}{2}$, lemma 6.1, and $\sigma\sqrt{t} \to 0$ for $t \to \infty$.
If $y_0 = \frac{\pi}{2\sigma\sqrt{t}} + 1$, then $\cos(\sigma y\sqrt{t}) \ge 0$ for $y = \lfloor \frac{\pi}{2\sigma\sqrt{t}} + \frac{1}{2} \rfloor + \frac{1}{2}$, quod non. Hence $y_0 < \frac{\pi}{2\sigma\sqrt{t}} + 1$, so y_0 is indeed a zero of F. □

Now we define G (again only in this section) by

$$G(y) = F(-y),$$

and z_0 to be the smallest zero of G in the interval $(0, y_0+1)$ provided such zeros exist; otherwise we define $z_0 = y_0+1$.
Then

$$G(-\tfrac{1}{2}) = G(\tfrac{1}{2}) = 1,$$

and, by the definition of B, G satisfies the difference equation

$$G(y+1) - B(y)G(y) + G(y-1) = 0.$$

LEMMA 3. $G(y) < F(y)$ *for* $y \in [\frac{1}{2}, z_0]_{\mathbb{Z}}$,

$$z_0 < y_0 + 1,$$

and

z_0 *is the smallest positive zero of* G.

PROOF. Similar to the proof of lemma 1, we start noting that
$z_0 \le y_0 + 1 \le \frac{5}{\sigma\sqrt{t}}$.

The first assertion of the lemma now follows from lemma 1.2 with $a = \frac{1}{2}$, $b = \lfloor z_0-\frac{1}{2}\rfloor+\frac{1}{2}$ and lemma 6.3. If $z_0 = y_0+1$, then $F(\lfloor y_0+\frac{1}{2}\rfloor+\frac{1}{2}) > 0$, which contradicts lemma 2. Hence $z_0 < y_0+1$, so z_0 is indeed a zero of G. □

Define y_0^* by $y_0^* = \lfloor y_0-\frac{1}{2}\rfloor+\frac{1}{2}$.

LEMMA 4. $F(y) \ge \frac{y_0^*-y_0}{y_0^*}$ *for* $y \in [\frac{1}{2},y_0^*]_{\mathbb{Z}}$.

PROOF. By lemma 7.2, F is positive on $[\frac{1}{2},y_0^*]_{\mathbb{Z}}$. If $y \in [\frac{1}{2},y_0^*]_{\mathbb{Z}}$, then $|y| \le \frac{5}{\sigma\sqrt{t}}$, so it follows from lemma 6.1 that $A(y) \le 2$. Hence, by the difference equation for F derived above, F is concave on $[\frac{1}{2},y_0^*]_{\mathbb{Z}}$. Moreover, $F(\frac{1}{2}) = 1$ and $F(y_0^*) \ge 0$. □

The following estimates hold in lemma 1.1 with $a = \frac{1}{2}$, $b = y_0^*-1$:

$$\alpha(k) \ll \sigma^3\sqrt{t}\cos(\sigma k\sqrt{t}) \le \sigma^3\sqrt{t}\, k \qquad \textit{for } k \in [\tfrac{1}{2},y_0^*-1]_{\mathbb{Z}},$$

$$\beta(k) \ll \sigma^3\sqrt{t} \sum_{i\in[\frac{1}{2},k)_{\mathbb{Z}}} 1 \le \sigma^3\sqrt{t}\, k \qquad \textit{for } k \in (\tfrac{1}{2},y_0^*-1]_{\mathbb{Z}},$$

$$\gamma(k) \ll \sum_{i\in(\frac{1}{2},k]_{\mathbb{Z}}} \frac{\sigma^3\sqrt{t}\, i\, y_0^{*2}}{(y_0^*-i)(y_0^*-i+1)} \le \sigma^3\sqrt{t}\, y_0^{*3} \ll \frac{1}{t} \qquad \textit{for } k \in [\tfrac{1}{2},y_0^*-1]_{\mathbb{Z}}.$$

Hence $\gamma(y) < 1$, so $G(y) > 0$ for $y \in [\frac{1}{2},y_0^*-1]_{\mathbb{Z}}$.

Consequently, $z_0 > y_0^*-1 > y_0-2$, so

LEMMA 5. $y_0-2 < z_0 < y_0+1$. □

Recapitulating, we know that M has zeros in x_0+y_0 and x_0-z_0 with $-\frac{3}{2} < x_0 < t$, $0 < y_0 < \frac{\pi}{2\sigma\sqrt{t}} + 1$, $z_0 > 0$, and $-1 < y_0 - z_0 < 2$.

Now define x_0' and y_0' by

$$x_0' = x_0 + \tfrac{1}{2}(y_0-z_0),$$

$$y_0' = \tfrac{1}{2}(y_0+z_0).$$

Then $-2 < x_0' < t+1$, $0 < y_0' < \frac{\pi}{2\sigma\sqrt{t}} + \frac{3}{2}$, and M has zeros in $x_0'+y_0'$ and $x_0'-y_0'$.

8. THE DISTANCE BETWEEN TWO CONSECUTIVE ZEROS

We return to the general case that t may be even as well as odd. If t is even, then we define x_0 and y_0 by $x_0 = x_0'$ and $y_0 = y_0'$, where x_0' and y_0' have been defined at the end of section 7. For t odd, x_0 is defined by

$$x_0 = \frac{q-1}{q} n - v_0,$$

where v_0 has been defined in lemma 3.3 with $k = t$, and y_0 by $y_0 = 0$.

Now by the end of section 7, respectively lemma 2.4:

<u>LEMMA 1</u>. $M(x_0+y_0) = M(x_0-y_0) = 0,$

$$-2 < x_0 < t+1,$$

$$0 \le y_0 < \frac{\pi}{2\sigma\sqrt{t}} + \frac{3}{2}. \quad \square$$

We recall that y, A and B have been defined in §6. We define F by

$$F(y) = \frac{M(x)}{M(x_0+y_0+1)},$$

and y_1 to be the smallest zero of F in the interval $(y_0, y_0+\lfloor\frac{\pi}{\sigma\sqrt{t}}\rfloor+1)$ provided such zeros exist; otherwise we define $y_1 = y_0+\lfloor\frac{\pi}{\sigma\sqrt{t}}\rfloor+1$.

Note that the zeros of F are simple and that their mutual distances are integers and at least 2 (cf. lemma 4.1). In particular

$$y_1 \in \mathbb{Z}+y_0,$$

and

$$y_1 \ge y_0+2.$$

Moreover

$$F(y_0) = \frac{M(x_0+y_0)}{M(x_0+y_0+1)} = 0,$$

$$F(-y_0) = \frac{M(x_0-y_0)}{M(x_0+y_0+1)} = 0,$$

and

$$F(y_0+1) = \frac{M(x_0+y_0+1)}{M(x_0+y_0+1)} = 1.$$

Finally, due to the definition of A and lemma 5.5, F satisies the difference equation

$$F(y+1) - A(y)F(y) + F(y-1) = 0.$$

LEMMA 2.

$$F(y) \ll \frac{\sin(\sigma(y-y_0)\sqrt{t})}{\sigma\sqrt{t}} \qquad \textit{for } y \in [y_0,y_1]_{\mathbb{Z}},$$

$$F(y) \gg \frac{\sin(2\sigma(y-y_0)\sqrt{t})}{\sigma\sqrt{t}} \qquad \textit{for } y \in [y_0,y_0+\frac{\pi}{2\sigma\sqrt{t}}]_{\mathbb{Z}},$$

$$\frac{\pi}{2\sigma\sqrt{t}} \le y_1 < \frac{3\pi}{2\sigma\sqrt{t}} + \frac{5}{2},$$

and

y_1 *is the smallest zero of* F *that exceeds* y_0.

PROOF. We first note that $y_1 \le y_0 + \frac{\pi}{\sigma\sqrt{t}} + 1 \le \frac{3\pi}{2\sigma\sqrt{t}} + \frac{5}{2} \le \frac{5}{\sigma\sqrt{t}}$.
If $G(y+1) - 2\cos(\sigma\sqrt{t})G(y) + G(y-1) = 0$, $G(y_0) = 0$, $G(y_0+1) = 1$, then

$$G(y) = \frac{\sin(\sigma(y-y_0)\sqrt{t})}{\sin(\sigma\sqrt{t})} \qquad \text{for } y \in \mathbb{Z} + y_0.$$

The first assertion of the lemma now follows from lemma 1.2 with $a = y_0+1$, $b = y_1$, lemma 6.1, and $\sigma\sqrt{t} \to 0$ for $t \to \infty$. The second assertion follows similarly. Obviously

$$\frac{\pi}{2\sigma\sqrt{t}} \le y_1-y_0 \le \frac{\pi}{\sigma\sqrt{t}} < \lfloor\frac{\pi}{\sigma\sqrt{t}}\rfloor+1.$$

So y_1 is indeed a zero of F and the third assertion follows from lemma 1. □

Now define G by

$$G(y) = \frac{F(-y)}{F(-y_0-1)},$$

and z_0 to be the smallest zero of G in the interval (y_0,y_1) if such zeros exist; otherwise define $z_1 = y_1$. Then

$$G(y_0) = 0,$$

$$G(y_0+1) = 1,$$

and

$$z_1 \in \mathbb{Z}+y_0.$$

Moreover, by the definition of B, G satisifes the difference equation

$$G(y+1) - B(y)G(y) + G(y-1) = 0.$$

LEMMA 3. $G(y) < F(y)$ *for* $y \in (y_0+1,z_1]_{\mathbb{Z}}$,

$z_1 < y_1$

and

z_1 *is the smallest zero of* G *that exceeds* y_0.

PROOF. As in the proof of lemma 2 we start noting that $z_1 \leq y_1 \leq \frac{5}{\sigma\sqrt{t}}$. The first assertion of the lemma now follows from lemma 1.2 with $a = y_0+1$, $b = z_1$, and lemma 6.3. The second one is obvious, so z_1 is indeed a zero of G. □

Define η by $\eta = y_0+\lfloor\frac{1}{2}(y_1-y_0)\rfloor$.

LEMMA 4. $F(y) \gg y-y_0$ *for* $y \in [y_0,\eta]_{\mathbb{Z}}$,

$F(y) \gg y_1-y$ *for* $y \in [\eta,y_1]_{\mathbb{Z}}$.

PROOF. The first assertion follows from lemma 2. Particularly, $F(\eta) \gg y_1-y_0$. Moreover, $F(y_1) = 0$ and F is concave on $[\eta,y_1]_{\mathbb{Z}}$ because $y_1 \leq \frac{5}{\sigma\sqrt{t}}$, so $A(y) \leq 2$ for $y \in [\eta,y_1]$ (cf. lemma 6.1). □

Now the following estimates hold in lemma 1.1 with $a = y_0+1$ and $b = y_1-1$:

$$\alpha(k) << \sigma^3\sqrt{t}\ \frac{\sin^2(\sigma(k-y_0)\sqrt{t})}{\sigma^2 t} << \sigma^3\sqrt{t}\ (k-y_0)^2 \quad \text{for } k \in [y_0+1, y_1-1)_{\mathbb{Z}},$$

$$\beta(k) << \sigma^3\sqrt{t} \sum_{i\in[y_0+1,k)_{\mathbb{Z}}} (k-y_0)^2 << \sigma^3\sqrt{t}(k-y_0)^3 \quad \text{for } k \in (y_0+1, y_1-1]_{\mathbb{Z}},$$

$$\gamma(k) << \sum_{i\in(y_0+1,\eta]_{\mathbb{Z}}} \frac{\sigma^3\sqrt{t}(i-y_0)^3}{(i-y_0)(i-y_0-1)} + \sum_{i\in(\eta,k]_{\mathbb{Z}}} \frac{\sigma^3\sqrt{t}(i-y_0)^3}{(y_1-i)(y_1-i+1)} \le$$

$$\le 2\sigma^3\sqrt{t}\ (y_1-y_0)^3 << \sigma^3\sqrt{t}\ y_1^3 << \frac{1}{t} \quad \text{for } k \in [y_0+1, y_1-1]_{\mathbb{Z}}.$$

Hence $\gamma(y) < 1$ so $G(y) > 0$ for $y \in [y_0+1, y_1-1]_{\mathbb{Z}}$.

Consequently, $z_1 > y_1-1$, so

LEMMA 5. $y_1-1 < z_1 < y_1$. □

However, lemma 5 contradicts $y_1 \in \mathbb{Z}+y_0$ and $z_1 \in \mathbb{Z}+y_0$. Hence our assumptions are contradictory.

9. CONCLUSION

In the previous sections we made several assumptions, which turned out to be contradictory. This proves

LEMMA 1. *Let* q, n, $t \in \mathbb{N}$, t *sufficiently large,* $q > 2$, $n \ge t$. *Then* K_t *has at least one non-integral zero.* □

We may combine this lemma with the famous theorem of LLOYD (lemma 2), for arbitrary alphabets proved by J. DELSARTE and H.W. LENSTRA jr. (cf. [6], [2] and [3]), with a theorem found recently by E. BANNAI (lemma 3, cf. [1]), and with the results of J.H. van LINT and A. TIETÄVÄINEN & A. PERKO on binary perfect codes (lemma 4, cf. [4], section 7.6 or [8]).

LEMMA 2. *If a* t-*perfect code of length* $n+1$ *over an alphabet of* q *symbols exists, then* K_t *has only integral zeros.* □

LEMMA 3. *For given* $t \ge 3$, *only finitely many* t-*perfect codes exist.* □

LEMMA 4. *The only binary perfect codes correcting at least two errors are the 3-perfect Golay code of length* 23 *and the repetition codes of odd length.* □

We get

THEOREM 1. *Besides the trivial codes and the binary repetition codes of odd length, only finitely many perfect codes correcting at least three errors exist.*

PROOF. From lemma 1 and 2 follows that for sufficiently large t, no t-perfect codes of length n+1 over an alphabet of q symbols exist, unless q = 2 or t > n. But q = 2 corresponds to binary codes, and t > n to trivial codes. Hence combination with lemma 3 and 4 yields the desired result. □

REFERENCES

1. BANNAI, EIICHI, *On Perfect Codes in the Hamming Schemes* H(n,q) *with* q *Arbitrary*, J. Comb. Theory (A) 23 (1977) 52-67.

2. DELSARTE, P., *Bounds for unrestricted codes, by linear programming*, Philips Res. Reports, 27 (1972) 272-289.

3. LENSTRA, Jr., H.W., *Two theorems on perfect codes*, Discrete Math. 3 (1972) 125-132.

4. LINT, J.H. van & H.C.A. van TILBORG, *Gelijkmatig verdeelde codes*, Chapter 7 in: J.H. van LINT (red.), *Inleiding in de coderingstheorie*, M.C. syllabus 31, Mathematisch Centrum, Amsterdam 1976 (in dutch).

5. LLOYD, S.P., *Binary block coding*, Bell Syst. Tech. J. 36 (1957) 517-535.

6. SZEGÖ, GABOR, *Orthogonal polynomials*, Amer. Math. Soc. Colloquium Publications, Vol. 23, New York, revised edition 1959.

7. TIETÄVÄINEN, A., *A short proof for the nonexistence of unknown perfect codes over* GF(q), q > 2, Ann. Acad. Sci. Fenn., Ser. A, (I. Mathematica), No. 580 (1974) 3-5.

8. TIETÄVÄINEN, A. & A. PERKO, *There are no unknown perfect binary codes*, Ann. Univ. Turku, Ser. A, 148 (1971) 3-10.