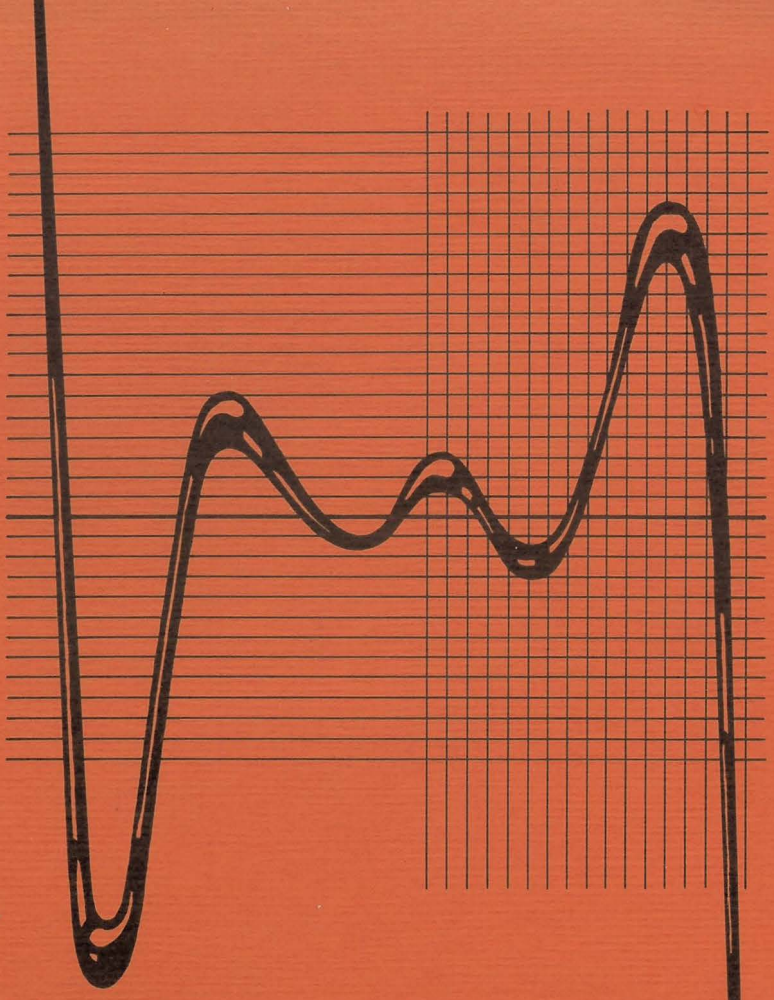


A CONTRIBUTION TO THE NONEXISTENCE OF PERFECT CODES

M.R. BEST

A CONTRIBUTION TO THE NONEXISTENCE OF PERFECT CODES

A CONTRIBUTION TO THE NONEXISTENCE OF PERFECT CODES

ACADEMISCH PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN
DOCTOR IN DE WISKUNDE IN NATUURWETENSCHAPPEN
AAN DE UNIVERSITEIT VAN AMSTERDAM
OP GEZAG VAN DE RECTOR MAGNIFICUS
Dr. D.W. BRESTERS
HOOGLERAAR IN DE FACULTEIT
DER WISKUNDE EN NATUURWETENSCHAPPEN
IN HET OPENBAAR TE VERDEDIGEN
IN DE AULA DER UNIVERSITEIT
(TIJDELIJK IN DE LUTHERSE KERK, INGANG SINGEL 411, HOEK SPUI)
OP WOENSDAG 2 JUNI 1982 DES NAMIDDAGS TE 1.30 UUR

DOOR

MARC ROELANT BEST

GEBOREN TE AMSTERDAM

PROMOTOR: PROF. DR. J.H. VAN LINT

COREFERENT: PROF. DR. J. KOREVAAR

ACKNOWLEDGEMENTS

I like to thank:

- the late Prof. dr. J. Popken, for guiding my first steps in scientific research;
- the Mathematical Centre, and in particular Prof. dr. P.C. Baayen, for enabling me to prepare this thesis and to cultivate other "nice mathematics", and for the willingness to publish this thesis so many years after I left;
- my former colleagues at the pure mathematics department, for the fruitful discussions we had, within and without W.G. Valiant;
- Prof. dr. J.H. van Lint, for encouraging me to study algebraic coding theory, and for repeatedly checking and amending the manuscript of this thesis, including the most tedious calculations;
- Eichii Bannai, for unknowingly, providing me with the basic idea of this thesis;
- the National Aerospace Laboratory NLR, for allowing me to finalize this thesis;
- Wout Loeve, for the rather abrupt, but very effective way he urged me to finish this job at long last;
- Hannu Laakso, for drawing my attention to several inaccuracies;
- José, for making the scarce sentences between the formulas into correct english;
- Susan Carolan, for typing all those horrible formulas with great accuracy;
- Tobias Baanders, for designing the cover;
- the publishing department of the Mathematical Centre, in particular Dick Zwarst and Jan Schippers for realizing this booklet in a very short time;
- Halley's comet, for coming along, in order to show me that coding theory is more than "nice mathematics".

CONTENTS

CHAPTER 1

INTRODUCTION

1.1. Perfect codes

One of the main aims of algebraic coding theory is to construct "good" "codes". These objects can be, and are, widely used in all sorts of communication systems, including satellite communication, telemetry, television, radar, magnetic tape, etc. etc. All these links have one thing in common, that being that a sender tries to transmit information to a receiver, but that during transmission errors are unavoidable.

Already since the time of papertape, it has been known that it is advisable to transmit more symbols than are strictly necessary. Thus only a small part of all thinkable strings is legitimate. Assuming that a message is encoded as a string consisting of a fixed number of symbols chosen from some fixed alphabet, the collection of legitimate strings is called a (*block*) *code*; a legitimate string is called a *codeword*.

If only a limited amount of energy is available for the transmission of the message, the redundancy in the message decreases the available amount of energy per symbol, thus increasing the a priori symbol error probability. On the other hand, the same redundancy enables the receiver to detect, or even correct, many error patterns: he selects that codeword which is "closest" to the received string. Usually, this will result in a nett reduction of the symbol error probability. It will be intuitively clear that in a "good" code the codewords should not be too close to each other: two close codewords can easily be confused.

In order to specify the concept of closeness, a distance function between two strings is introduced. This (Hamming) distance is defined as the number of symbols by which two strings differ.

Consider, as an example, the code consisting of only two codewords, 00000 and 11111. Each codeword consists of five bits (zeros or ones). It is therefore called a binary code of block length five. It will be obvious

that - as long as a codeword is not corrupted by more than two errors - the receiver is able to reconstruct the transmitted codeword by "majority vote". For this reason, the code is called 2-error correcting. Geometrically, this means that the spheres with radius two around the codewords do not intersect. Each such sphere consists of the relevant codeword, together with all strings at distances one or two from the codeword.

A pecularity of the exemplary code is that not a single pattern of three or more errors can be corrected or even detected properly. This means that there is no room between the previously mentioned spheres. For this reason, the code is called 2-perfect. In general, a code is called t-*perfect* if the spheres with radius t around the codewords form a partitioning of the space of all thinkable strings of the relevant length over the relevant alphabet.

Trivial examples of t-perfect codes are the codes consisting of only one codeword of length at most t, and the binary repetition codes of block-length 2t+1, consisting of two codewords at distance 2t+1 apart. The codes consisting of *all* strings of a certain length over a certain alphabet are obviously 0-perfect.

Apart from these silly codes, an infinite class of 1-perfect codes was described by R.W. HAMMING in 1950 (cf. [8]). These codes contain 2^{n-r} codewords of length $n = 2^r-1$. The smallest nontrivial example (r=3, n=7) consists of the codewords 0000000, 1101000, 0010111, 1111111, and all cyclic shifts. Furthermore, a 3-perfect binary code consisting of 4096 codewords of length 23 was discovered by M.J.E. GOLAY in 1949 (cf. [7]). No more perfect binary codes were able to be discovered.*) Building on the work of J.H. van LINT (cf. [15]), A. TIETÄVÄINEN & A. PERKO [30] succeeded in proving that no more perfect binary codes existed indeed.

The class of Hamming codes is not confined to binary codes. For each alphabet with q symbols, q being a power of a prime, and each positive integer r, a 1-perfect code exists containing q^{n-r} codewords of length $n = (q^r-1)/(q-1)$. The smallest nontrivial example (q=3, r=2, n=4) is the ternary code consisting of the codewords 0000, 0111, 0222, 1012, 1120, 1201, 2021, 2102, 2210. Apart from this class, M.J.E. GOLAY also discovered a ternary 2-perfect code consisting of 729 codewords of length 11 (cf. [7]). No more perfect codes were able to be discovered.*)

*) Strictly speaking, this is not true: many 1-perfect codes have been discovered which have the same parameters as the Hamming codes, but are not equivalent to the Hamming codes. This holds for binary as well as for non-binary codes (cf. [31], [24], [11] and [33]).

After this poor yield, several researchers tried to prove that no more t-perfect codes over arbitrary alphabets existed indeed. The principal tools available for such nonexistence proofs are the "sphere packing condition", and "Lloyd's theorem". The sphere packing condition expresses that the number of strings in a sphere with radius t should be a divisor of the total number of strings; Lloyd's theorem relates the existence of a perfect code to the integrality of the zeros of a certain polynomial of degree t.

The nonexistence proof of unknown perfect binary codes was based on a combination of both tools. This technique has been refined and generalized in several papers ([12], [27], [13], [14], [15], [28], [17], [29], [2], [9]). The limitation of this proof technique is the use of the sphere packing condition. This divisibility criterion becomes weaker and weaker accordingly as the alphabet size gets more prime divisors. Therefore, a general nonexistence proof cannot be expected in this way.

The first nonexistence proof of perfect codes over arbitrary alphabets was published by H.F.H. REUVERS [22], who proved that unknown 3-, 4-, and 5- perfect codes do not exist. Later, E. BANNAI [1] proved that for any *fixed* $t \geq 3$ the number of t-perfect codes is finite. This was improved by M.R. BEST [4], who showed that the total number of unknown perfect codes correcting at least three errors is finite.

In this thesis, it will be proved that unknown perfect codes do not exist at all for $t \geq 3$, unless $t = 6$ or $t = 8$. Although the general "Perfect Code Theorem" - which states that no t-perfect codes exist apart from the known ones - could not be proved, the proof becomes apparent for the case $t \geq 3$. For the cases $t = 1$ and $t = 2$, the techniques developed in this thesis do not apply.

1.2. An outline of the proof

The discussion in this section is meant to give some insight into the main lines of the proof of the perfect code theorem, as will be attempted in this thesis. This discussion will be very informal, and should not be judged according to mathematical rigour. We hope it will give the reader a guided tour through the lengthy, but (hopefully) mathematically rigourous derivations in the subsequent chapters.

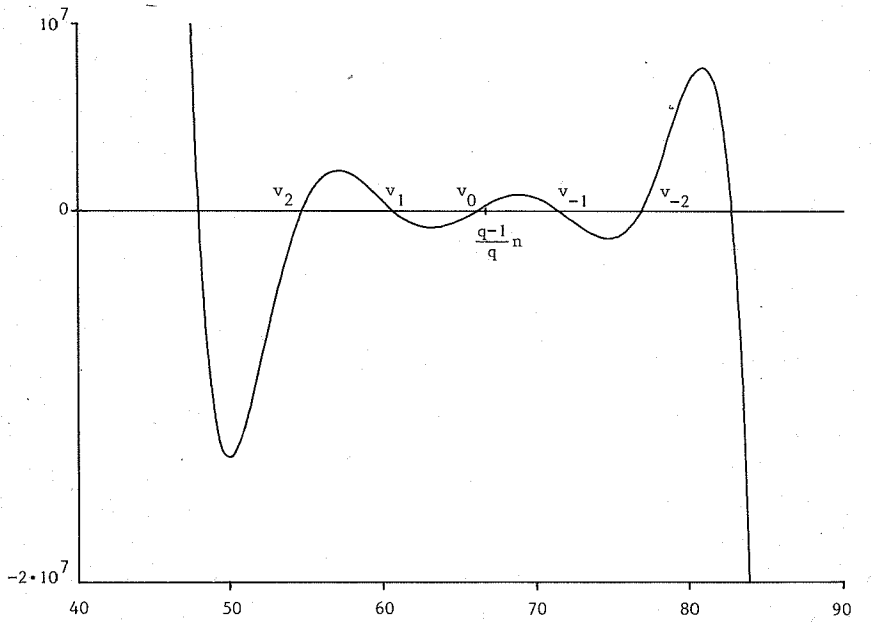
The theorem that will be proved is formulated in Chapter 9. It claims that no unknown t-perfect codes exist, unless t equals 1, 2, 6, or 8. These four exceptional cases are also discussed briefly in Chapter 9.

In the proof, two cases are distinguished: Chapters 5, 6, and 7 deal with the case of a relatively large block length, while Chapter 8 treats the case of a relatively small block length.

The proof of either case makes use of "Lloyd's theorem", which states that the existence of a certain t-perfect code implies that all zeros of a certain Kravčuk polynomial K_t^v are integral. S.P. Lloyd, in fact, proved this theorem only for linear binary codes. It was generalized by F.J. MacWilliams, P. Delsarte, and H.W. Lenstra jr. to general codes. This generalization, as well as other known results applying to perfect codes, is discussed in Chapter 4.

The exact definition of the Kravčuk polynomial K_t^v can be found in Chapter 3. In that chapter, the relevant properties of Kravčuk polynomials will also be derived. Chapter 2 contains a rather incoherent collection of notations and auxiliary results.

Consider, as an example, a t-perfect code with t odd ($t \geq 5$). The existence of such a code implies that a certain Kravčuk polynomial K_t^v has integral zeros. The graph of K_t^v is sketched below



The graph of K_t^v for t=7, n=100, q=3.

Here n equals the block length of the code decreased by one, and q denotes the alphabet size. For large values of the parameter n, the

graph tends - after some scaling - to that of a Hermite polynomial. This fact was used by E. Bannai to prove that for each *fixed* value of t only finitely many t-perfect codes exist. In his proof, the crucial observation is that the zeros of K_t are grouped *almost* symmetrically around a central zero v_0. In particular, the two adjacent zeros v_1 and v_{-1} of this central zero are *almost* equidistant from v_0.

In this thesis, the last statement will be specified precisely:

$$0 < (v_0-v_1) - (v_{-1}-v_0) < 1$$

for n larger than some well defined bound. This clearly contradicts the integrality of v_1, v_0 or v_{-1}.

In order to prove the above inequality, the Kravčuk polynomial K_t is studied in detail in the neighbourhood of v_0. This is done in three steps:

1. First, v_0 is estimated by expanding K_t in a neighbourhood of $(q-1)n/q$. This is done in Chapter 5.
2. Second, the (scaled) Kravčuk polynomial is approximated by an ordinary sine function (instead of a Hermite polynomial) in the neighbourhood of v_0. This is performed by using a difference equation (Lemma 3.3.1), valid for Kravčuk polynomials. This leads to a coarse estimate for the distance of consecutive zeros of Kravčuk polynomials (Lemma 6.3.1).
3. Third, the Kravčuk polynomial is compared to its own mirror-image with respect to v_0. Here again, the difference equation is employed. Since the scaled polynomial is almost antisymmetric around v_0, the difference equation is almost invariant under this reflection. This will enable us in Section 6.3 to estimate $(v_0-v_1) - (v_{-1}-v_0)$ with the promised accuracy.

In this example, t was chosen to be odd. In case t is even, there is no "central" zero. There is, however, some centre, close to $(q-1)n/q$, with respect to which the zeros of K_t are situated almost symmetrically. Similar to the odd case, it is possible to prove that

$$0 < (v_1-v_2) - (v_{-2}-v_{-1}) < 1,$$

where v_2, v_1, v_{-1}, and v_{-2} denote the four zeros surrounding this centre, in increasing order. This gives rise to several technical complications, which are dealt with in Chapter 7.

Finally, perfect codes with a relatively short block length will be ruled out by a system of divisibility relations (Lemma 8.1.1), which gen-

eralizes many formulas expressing that the product, the sum, the sum of the squares, etc., of the zeros of Lloyd's polynomial are integers. This system is very restrictive for not too large values of the block length. Without much effort, the nonexistence of such perfect codes can be shown.

CHAPTER 2

PRELIMINARIES

In this chapter, a number of notations are introduced and several results are derived which will be used in the subsequent chapters.

2.1. Notations

Some notations are listed below which will be used throughout this thesis, and which might be non-standard. In this section, a and b are real numbers, while j and k are integers.

$\mathbb{N}$ denotes the natural numbers, including zero.

$|C|$ denotes the cardinality of the set C.

$[a,b]$, $(a,b]$, $[a,b)$, and (a,b) denote closed, left-open, right-open, and open real intervals.

$[a,1,b]$, $(a,1,b]$, $[a,1,b)$, and $(a,1,b)$ denote the corresponding real intervals, intersected by $\mathbb{Z} + a$. E.g.

$$(a,1,b] = \{x | x \in (a,b] \wedge x-a \in \mathbb{Z}\}.$$

Weakly positive means positive or zero. (The author abhors the double negation "non-negative".) Likewise, *weakly negative* means negative or zero.

Increasing and decreasing are used in the weak sense.

$\lfloor a \rfloor$ denotes the greatest integer less than or equal to a.

$\lceil a \rceil$ denotes the least integer greater than or equal to a.

$a|b$ means that b is an integral multiple of a.

lcm(a,b) denotes the least positive real number that is an integral multiple of both a and b, provided such a number exists. Otherwise, lcm(a,b) = 0.

If $a > b$, then $\int_{t=a}^{b} f\, dt$ is defined as $-\int_{t=b}^{a} f\, dt$.

log denotes the natural logarithm.

a! denotes $\Gamma(a+1)$, where Γ is Euler's gamma function.

$a^{(j)}$ denotes $\prod_{i=0}^{j-1} (a+i)$ if $j \geq 0$.

$a_{(j)}$ denotes $\prod_{i=0}^{j-1} (a-i)$ if $j \geq 0$.

$\binom{a}{j}$ denotes $a_{(j)}/j!$ if $j \geq 0$; otherwise $\binom{a}{j} = 0$.

$\delta_{j,k}$ denotes Kronecker's δ-symbol.

$B(f)$ denotes some variable which is bounded above in absolute value by f. E.g. $\sin(x) = B(1)$. It is used in the same (questionable) manner as the Landau-Bachman O-symbol, with the difference being no multiplicative constant is involved.

□ denotes the end of a proof.

2.2. Various (in-)equalities

Since we prefer not to interrupt the proofs in the subsequent chapters by technical details, several identities and estimates are proved in this section for later reference.

LEMMA 2.2.1. *Let* $|x| < 1$. *Then*

$$\log(1+x) = x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3(1+B(|x|))^{-1}.$$

PROOF. For $x \geq 0$ as well as for $x < 0$ one has

$$\int_{y=0}^{x} \frac{3y^2+2y^3}{3(1+y)^2}\,dy \leq \int_{y=0}^{x} \frac{y^2}{1+y}\,dy \leq \int_{y=0}^{x} y^2 dy.$$

Hence

$$\frac{x^3}{3(1+x)} \leq \log(1+x) - x + \tfrac{1}{2}x^2 \leq \tfrac{1}{3}x^3. \quad \square$$

LEMMA 2.2.2. *Let* $n \in \mathbb{N}$. *Then*

$$\sum_{k=0}^{n-1} k^2 \leq \tfrac{1}{3}n^2(n-1),$$

and

$$\sum_{k=0}^{n-1} k^3 \le \tfrac{1}{4}n^3(n-1).$$

PROOF. This follows from $\sum_{k=0}^{n-1} k^2 = \frac{1}{6}n(n-1)(2n-1)$ and $\sum_{k=0}^{n-1} k^3 = \frac{1}{4}n^2(n-1)^2$. □

LEMMA 2.2.3. *Let* $n \in \mathbb{N}$ *and* $\omega \in \mathbb{R}$. *Then*

$$\sum_{k=1}^{n} \sin^2(k\omega) = \tfrac{1}{2}n - \frac{\sin(n\omega)\cos((n+1)\omega)}{2\sin\omega},$$

and

$$\sum_{k=1}^{n} k\sin^2(k\omega) = \tfrac{1}{4}n^2 - \frac{n\sin(n\omega)\cos((n+1)\omega)}{2\sin\omega} + \frac{\sin^2(n\omega)}{4\sin^2\omega},$$

provided $\omega \not\equiv 0 \pmod{\pi}$.

PROOF. According to exercise no. 16 in Chapter 6 of POLYA & SZEGÖ [21], one has for $\omega \not\equiv 0 \pmod{\pi}$:

$$\sum_{k=1}^{n} \cos(2k\omega) = \frac{\sin(n\omega)\cos((n+1)\omega)}{\sin\omega};$$

and

$$\sum_{k=1}^{n} (n+1-k)\cos(2k\omega) = \frac{\sin^2((n+1)\omega)}{2\sin^2\omega} - \frac{n+1}{2}.$$

The two formulas in the lemma follow straightforwardly. □

LEMMA 2.2.4. *Let* $\omega > 0$. *Then*

$$\sum_{k=1}^{\lfloor \pi/\omega \rfloor} \sin^2(k\omega) \le \tfrac{1}{2}\lceil \pi/\omega \rceil,$$

and

$$\sum_{k=1}^{\lfloor \pi/\omega \rfloor} k\sin^2(k\omega) \le \tfrac{1}{4}\lceil \pi/\omega \rceil^2.$$

PROOF. For $\omega > \pi$ as well as for $\frac{1}{2}\pi < \omega \le \pi$, the inequalities are verified directly. If $0 < \omega \le \frac{1}{2}\pi$ and $\pi/\omega \in \mathbb{Z}$, the inequalities follow at once from Lemma 2.2.3 (even with equality).

Now suppose that $0 < \omega \le \frac{1}{2}\pi$ and that $\pi/\omega \notin \mathbb{Z}$. Then

$$\tfrac{1}{2}\pi \le \pi - \omega \le \lfloor \pi/\omega \rfloor \omega \le \pi,$$

so

$$\sin(\lfloor \pi/\omega \rfloor \omega) \le \sin(\pi - \omega) = \sin \omega.$$

Lemma 2.2.3 (with $n = \lfloor \pi/\omega \rfloor$) yields

$$\sum_{k=1}^{\lfloor \pi/\omega \rfloor} \sin^2(k\omega) \le \tfrac{1}{2}\lfloor \pi/\omega \rfloor + \tfrac{1}{2} = \tfrac{1}{2}\lceil \pi/\omega \rceil,$$

and

$$\sum_{k=1}^{\lfloor \pi/\omega \rfloor} k \sin^2(k\omega) \le \tfrac{1}{4}\lfloor \pi/\omega \rfloor^2 + \tfrac{1}{2}\lfloor \pi/\omega \rfloor + \tfrac{1}{4} = \tfrac{1}{4}\lceil \pi/\omega \rceil^2,$$

respectively. □

LEMMA 2.2.5. *Let* $\omega > 0$. *Then*

$$\sum_{k=2}^{\lfloor \pi/(2\omega) \rfloor} \frac{1}{\sin(k\omega)\sin((k-1)\omega)} \le \frac{1}{\omega^2}.$$

PROOF. It can be assumed that $\omega < \frac{1}{2}\pi$. Let $n = \lfloor \pi/(2\omega) \rfloor$. Then

$$\sum_{k=2}^{n} \frac{1}{\sin(k\omega)\sin((k-1)\omega)} =$$

$$= \sum_{k=2}^{n} \frac{\sin(k\omega)\cos((k-1)\omega) - \cos(k\omega)\sin((k-1)\omega)}{\sin \omega \sin(k\omega)\sin((k-1)\omega)} =$$

$$= \frac{1}{\sin \omega} \sum_{k=2}^{n} (\cot((k-1)\omega) - \cot(k\omega)) =$$

$$= \frac{\cot \omega - \cot(n\omega)}{\sin \omega} \le \frac{1}{\sin \omega \tan \omega} \le \frac{1}{\omega^2}. \quad \square$$

In the next lemma, B_k denotes the k-th Bernoulli number, as defined in WHITTAKER & WATSON [32], §7.2. In particular, $B_1 = 1/6$, and $B_2 = 1/30$.

LEMMA 2.2.6. *Let* $n \in \mathbb{N}$, *and* $v > 0$. *Then*

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

$$= -\frac{1}{2}\log(\tfrac{1}{2}v) + \sum_{k=1}^{n} \frac{(-1)^k(4^k-1)B_k}{(2k)(2k-1)v^{2k-1}} - \frac{(-1)^n}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+v^2} \frac{dt}{\sinh(\pi t)} .$$

Moreover,

$$-\frac{1}{2}\log(\tfrac{1}{2}v) + \sum_{k=1}^{n} \frac{(-1)^k(4^k-1)B_k}{(2k)(2k-1)v^{2k-1}}$$

is an upper (a lower) bound for $\log \frac{(\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!}$ *if* n *is even (odd). In particular,*

$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!} = -\frac{1}{2}\log(\tfrac{1}{2}v) + \mathcal{B}(\frac{1}{4v}),$$

and

$$\log \frac{(\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!} = -\frac{1}{2}\log(\tfrac{1}{2}v) - \frac{1}{4v} + \mathcal{B}(\frac{1}{24v^3}).$$

PROOF. From Stirling's asymptotic expansion of the logarithm of the gamma function (cf. WHITTAKER & WATSON [32], §12.33), it is known that

$$\log \Gamma(v) = (v-\tfrac{1}{2})\log v - v + \tfrac{1}{2}\log(2\pi) + \sum_{k=1}^{n} \frac{(-1)^{k-1}B_k}{(2k)(2k-1)v^{2k-1}} + \frac{2(-1)^n}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+v^2} \frac{dt}{e^{2\pi t}-1} .$$

Hence

$$\log v! = \log \Gamma(v) + \log v =$$

$$= (v+\tfrac{1}{2})\log v - v + \tfrac{1}{2}\log(2\pi) + \sum_{k=1}^{n} \frac{(-1)^{k-1}B_k}{(2k)(2k-1)v^{2k-1}} + R_1,$$

where

$$R_1 = \frac{2(-1)^n}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+v^2} \frac{dt}{e^{2\pi t}-1} .$$

Moreover,

$$2\log(\tfrac{1}{2}v)! =$$

$$= (v+1)\log(\tfrac{1}{2}v) - v + \log(2\pi) + \sum_{k=1}^{n} \frac{(-1)^{k-1}2^{2k}B_k}{(2k)(2k-1)v^{2k-1}} + R_2,$$

where

$$R_2 = \frac{2(-1)^n 2^{2n}}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+\frac{1}{4}v^2} \frac{dt}{e^{2\pi t}-1} =$$

$$= \frac{2(-1)^n}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+v^2} \frac{dt}{e^{\pi t}-1} .$$

Hence

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

$$= -\frac{1}{2}\log(\tfrac{1}{2}v) + v \log 2 - \frac{1}{2}\log \pi + \sum_{k=1}^{n} \frac{(-1)^k(4^k-1)B_k}{(2k)(2k-1)v^{2k-1}} + R,$$

where

$$R = R_1 - R_2 = -\frac{(-1)^n}{v^{2n-1}} \int_{t=0}^{\infty} \int_{u=0}^{t} \frac{u^{2n}du}{u^2+v^2} \frac{dt}{\sinh(\pi t)} .$$

According to the Legendre duplication formula (cf. WHITTAKER & WATSON [32], §12.15),

$$\Gamma(z)\Gamma(z+\tfrac{1}{2}) = \pi^{\frac{1}{2}} 2^{1-2z} \Gamma(2z),$$

which transforms easily into

$$(\tfrac{1}{2}v)! \, (\tfrac{1}{2}v - \tfrac{1}{2})! = \pi^{\frac{1}{2}} 2^{-v} v!.$$

Hence,

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

$$= -\frac{1}{2}\log(\tfrac{1}{2}v) + \sum_{k=1}^{n} \frac{(-1)^k(4^k-1)B_k}{(2k)(2k-1)v^{2k-1}} + R,$$

proving the first part of the lemma.

The upper (lower) bound follows since R is negative (positive) for n even (odd).

The particular cases are found by taking respectively n=0, n=1, and n=2. □

2.3. Logarithmically concave sequences

A real sequence $(a_i)_{i=0}^{\infty}$ is called *logarithmically concave*, or briefly *logconcave*, if it is weakly positive and moreover

$$a_k a_{\ell+1} \leq a_{k+1} a_\ell$$

for all $k \in \mathbb{N}$ and $\ell \in \mathbb{N}$ with $k \leq \ell$. In this case we also say that a_i is *logconcave in* i *for* $i \in \mathbb{N}$. A trivial consequence of the definition is mentioned in the next lemma.

LEMMA 2.3.1. *Let* $(a_i)_{i=0}^{\infty}$ *be concave. Then*

$$a_k a_{\ell+j} \leq a_{k+j} a_\ell$$

for all $j \in \mathbb{N}$, $k \in \mathbb{N}$, *and* $\ell \in \mathbb{N}$ *with* $k \leq \ell$.

PROOF. By induction with respect to j. □

In the definition we adopted, zero terms are allowed. These can occur however only at the beginning or the end of the sequence, as is shown by the next lemma.

LEMMA 2.3.2. *Let* $(a_i)_{i=0}^{\infty}$ *be a real sequence. Then it is logconcave if and only if the following three conditions are satisfied:*

1. $a_i \geq 0$ *for all* $i \in \mathbb{N}$;
2. *if* $k \in \mathbb{N}$, $\ell \in \mathbb{N}$, $a_k > 0$, *and* $a_\ell > 0$, *then* $a_i > 0$ *for all* $i \in [k,1,\ell]$;
3. $a_i^2 \geq a_{i-1}\, a_{i+1}$ *for all* $i \in \mathbb{N} \setminus \{0\}$.

PROOF. Suppose that $(a_i)_{i=0}^{\infty}$ is logconcave. Then the first and third condition are obvious. The second condition follows from Lemma 2.3.1:

$$0 < a_k a_\ell \leq a_i a_{k+\ell-i},$$

provided $i \in [k,1,\ell]$.

Next suppose that the three conditions are met. Suppose that $k \in \mathbb{N}$, $\ell \in \mathbb{N}$, and $k \leq \ell$. It should be proved that $a_k a_{\ell+1} \leq a_{k+1} a_\ell$.

If $a_k a_{\ell+1} = 0$, the assertion is obvious, so it can be assumed that $a_k > 0$ and $a_{\ell+1} > 0$. But then $a_i > 0$ for all $i \in [k,1,\ell+1]$. Also

$$\prod_{i=k+1}^{\ell} a_i^2 \geq \prod_{i=k+1}^{\ell} (a_{i+1}a_{i-1}) = a_k a_{k+1} a_\ell a_{\ell+1} \prod_{i=k+2}^{\ell-1} a_i^2,$$

so

$$a_{k+1}a_\ell \geq a_k a_{\ell+1},$$

which was to be proved. □

It is obvious from the definition that the product of two logconcave sequences is again logconcave.

LEMMA 2.3.3. *Let* $(a_i)_{i=0}^{\infty}$ *and* $(b_i)_{i=0}^{\infty}$ *be logconcave sequences. Then* $(a_i b_i)_{i=0}^{\infty}$ *is logconcave as well.*

It is less obvious that the convolution product of two logconcave sequences is again logconcave. This is stated in the next lemma.

LEMMA 2.3.4. *If the coefficients of the power series* f *and* g *both form logconcave sequences, then the coefficients of the Cauchy product* fg *form a logconcave sequence as well.*

PROOF. Let $f(X) = \Sigma_{i=0}^{\infty} a_i X^i$, $g(X) = \Sigma_{i=0}^{\infty} b_i X^i$, and $(fg)(X) = \Sigma_{k=0}^{\infty} c_k X^k$. Then $c_k = \Sigma_{i=0}^{k} a_i b_{k-i}$. It can easily be checked that $(c_k)_{k=0}^{\infty}$ meets the first two conditions of Lemma 2.3.2. Next, define $a_{-1} = b_{-1} = 0$. From the logconcavity of $(a_i)_{i=0}^{\infty}$ and $(b_i)_{i=0}^{\infty}$ it follows that

$$a_i a_{j-1} \geq a_{i-1}a_j \text{ and } b_{k-i}b_{k+1-j} \geq b_{k+1-i}b_{k-j} \text{ if } i \leq j \leq k+1$$

and

$$a_i a_{j-1} \leq a_{i-1}a_j \text{ and } b_{k-i}b_{k+1-j} \leq b_{k+1-i}b_{k-j} \text{ if } j \leq i \leq k+1$$

for $i \in \mathbb{N}$, $j \in \mathbb{N}$, and $k \in \mathbb{N}$. Hence

$$c_k^2 - c_{k+1}c_{k-1} =$$

$$= \Big(\sum_{i=0}^{k+1} a_i b_{k-i}\Big)\Big(\sum_{j=0}^{k+1} a_{j-1}b_{k+1-j}\Big) - \Big(\sum_{i=0}^{k+1} a_i b_{k+1-i}\Big)\Big(\sum_{j=0}^{k+1} a_{j-1}b_{k-j}\Big) =$$

$$= \sum_{i=0}^{k+1} \sum_{j=0}^{k+1} a_i a_{j-1} (b_{k-1} b_{k+1-j} - b_{k+1-i} b_{k-j}) =$$

$$= \frac{1}{2} \sum_{i=0}^{k+1} \sum_{j=0}^{k+1} (a_i a_{j-1} (b_{k-i} b_{k+1-j} - b_{k+1-i} b_{k-j}) +$$

$$+ a_j a_{i-1} (b_{k-j} b_{k+1-i} - b_{k+1-j} b_{k-i})) =$$

$$= \frac{1}{2} \sum_{i=0}^{k+1} \sum_{j=0}^{k+1} (a_i a_{j-1} - a_{i-1} a_j)(b_{k-i} b_{k+1-j} - b_{k+1-i} b_{k-j}) \geq 0.$$

This proves the third condition of Lemma 2.3.2. □

Finally, a more complicated result can be shown.

LEMMA 2.3.5. *Let* $(\beta(j))_{j=0}^{\infty}$ *be a logconcave sequence, and let*

$$b_{k,c} = \sum_{\substack{j_1,\ldots,j_c=0 \\ j_1+\ldots+j_c=k}}^{\infty} \prod_{i=1}^{c} \beta(j_i).$$

Then $b_{k,c}$ *is logconcave in* k *as well as in* c.

PROOF. Since

$$\sum_{k=0}^{\infty} b_{k,c} X^k = \sum_{j_1,\ldots,j_c=0}^{\infty} \prod_{i=1}^{c} (\beta(j_i) X^{j_i}) = \Big(\sum_{j=0}^{\infty} \beta(j) X^j\Big)^c,$$

Lemma 2.3.4 yields that $b_{k,c}$ is logconcave in k.

The first condition of Lemma 2.3.2 (with $(a_i)_{i=0}^{\infty} = (b_{k,c})_{c=0}^{\infty}$) is obviously met.

Next, let $c \in \mathbb{N}$, $d \in \mathbb{N}$, $b_{k,c} > 0$, $b_{k,d} > 0$, and $i \in [c,1,d]$. Then according to the definition of $b_{k,c}$, there should be an $\ell \geq \lceil k/c \rceil$ such that $\beta(\ell) > 0$. Similarly, there should be an $m \leq \lfloor k/d \rfloor$ such that $\beta(m) > 0$. Since β is logconcave, and $\lfloor k/d \rfloor \leq \lfloor k/i \rfloor \leq \lceil k/i \rceil \leq \lceil k/c \rceil$, this implies that $\beta(\lfloor k/i \rfloor)$ and $\beta(\lceil k/i \rceil)$ are positive. Therefore,

$$b_{k,i} \geq \beta^i(k/i) > 0 \qquad \text{if } i \mid k$$

and

$$b_{k,i} \geq \beta^{i\lceil k/i \rceil - k}(\lfloor k/i \rfloor) \beta^{k-i\lfloor k/i \rfloor}(\lceil k/i \rceil) > 0 \qquad \text{if } i \nmid k$$

This proves the second condition in Lemma 2.3.2.

From the definition of $b_{k,c}$ it is clear that

$$b_{k,c} = \sum_{j=0}^{\infty} \beta(j)\, b_{k-j,c-1},$$

so

$$b_{k,c+1} = \sum_{i=0}^{\infty} \beta(i) b_{k-i,c} = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \beta(i)\beta(j) b_{k-i-j,c-1},$$

and

$$b_{k,c}^2 = \Big(\sum_{j=0}^{\infty} \beta(j) b_{k-j,c-1}\Big)^2 = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \beta(i)\beta(j) b_{k-i,c-1} b_{k-j,c-1}.$$

Since $b_{k,c-1}$ is logconcave in k, Lemma 2.3.1 yields:

$$b_{k-i,c-1} b_{k-j,c-1} \geq b_{k,c-1} b_{k-i-j,c-1},$$

so

$$b_{k,c}^2 \geq \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \beta(i)\beta(j) b_{k,c-1} b_{k-i-j,c-1} = b_{k,c-1} b_{k,c+1}.$$

This proves the lemma. □

It will be obvious that for finite sequences logconcavity can be defined completely analogously to logconcavity for infinite sequences, and that similar results hold.

2.4. Three term recurrence relations

In this section, estimates are derived for the solution of a recurrence relation of the type

$$F(k+1) - A(k)F(k) + R(k)F(k-1) = 0,$$

in which R does not vanish anywhere. First, the relation is simplified by the substitution F = gG, where g is a function which has no zeros, and which satisfies the two term recurrence relation

$$g(k+1) = R(k)g(k-1).$$

(Of course, many such functions g exist.) Now

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

so

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

where

$$B(k) = \frac{A(k)g(k)}{g(k+1)} .$$

In the next four lemmas, the effect of a perturbation on the function B is analysed. In view of later applications, k is not restricted to $\mathbb{Z}$ (which is obviously allowed), but it assumes values in $\mathbb{Z}+a$ for some $a \in \mathbb{R}$. The lemmas regain their natural form by taking a = 1.

LEMMA 2.4.1. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z}+a$, *and let* F, G, A, *and* B *be real functions so that*

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

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

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

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

$$F(k) \neq 0 \quad \textit{for } k \in [a,1,b].$$

Then

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

where

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

$$\beta(k) = \sum_{i\in[a,1,k)} \alpha(i) \quad \textit{for } k \in [a,1,b],$$

$$\alpha(k) = (A(k) - B(k))F(k)G(k) \qquad \textit{for } k \in [a,1,b).$$

PROOF. Two identities are proved simultaneously for $k \in [a,1,b]$:

$$F(k)G(k-1) - F(k-1)G(k) = \beta(k)$$

and

$$G(k) = (1-\gamma(k))F(k).$$

For $k = a$, the identities are obvious. Assume that they have been proved for certain $k \in [a,1,b)$. 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

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

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

This proves the lemma by induction. □

The following lemma proves that, under certain initial conditions, the solution of a recurrence relation is strictly bounded by the solution of another relation of the same kind.

LEMMA 2.4.2. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z} + a$, *and let* F, G, A, *and* B *be real functions so that*

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

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

$$F(a+1)G(a) < F(a)G(a+1),$$

$$F(a+1) < G(a+1),$$

$$F(k) > 0 \qquad \textit{for } k \in (a,1,b),$$

$$F(b) \geq 0,$$

$$A(k) \leq B(k) \qquad \textit{for } k \in (a,1,b).$$

Then

$$F(k) < G(k) \qquad \textit{for } k \in (a,1,b].$$

PROOF. Two inequalities are proved simultaneously for $k \in (a,1,b]$:

$$F(k)G(k-1) < F(k-1)G(k),$$

and

$$F(k) < G(k).$$

For $k = a+1$, the inequalities are given. Assume that they have been proved for certain $k \in (a,1,b)$. Then

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

$$= (A(k) - B(k))F(k)G(k) + F(k)G(k-1) - F(k-1)G(k) < 0.$$

From this it is clear that $G(k+1) > 0$, so

$$F(k+1)G(k) < F(k)G(k+1) < G(k)G(k+1),$$

which implies

$$F(k+1) < G(k+1). \quad \square$$

In view of later applications, the following consequence of Lemma 2.4.2 is proved

LEMMA 2.4.3. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z} + a$, *and let* F, G, A, *and* B *be real functions so that*

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

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

$$F(a-1) \geq G(a-1),$$

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

$$F(a-1) \geq 0,$$

$$F(k) > 0 \qquad \text{for } k \in [a,1,b),$$

$$F(b) \geq 0,$$

$$A(a) < B(a),$$

$$A(k) \leq B(k) \qquad \text{for } k \in (a,1,b).$$

Then

$$F(k) < G(k) \qquad \text{for } k \in (a,1,b].$$

PROOF. It can be assumed that $b \geq a+1$. Then

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

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

Hence

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

At this stage, one easily checks that all conditions in Lemma 2.4.2 have been complied with. □

Finally, an analogue to Lemma 2.4.2 is proved in which inequalities are given at both boundaries.

LEMMA 2.4.4. *Let* $a \in \mathbb{R}$, $b \in \mathbb{Z} + a$, *and let* F, G, A, *and* B *be real functions so that*

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

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

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

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

$$F(k) > 0 \qquad \textit{for } k \in [a,1,b),$$

$$F(b) \geq 0,$$

$$A(k) \leq B(k) \qquad \textit{for } k \in (a,1,b).$$

Then

$$F(k) \geq G(k) \qquad \textit{for } k \in [a,1,b].$$

PROOF. It can be assumed that $a \leq b$. Let a' be the largest number in $[a,1,b]$ for which $F(k) \geq G(k)$ for $k \in [a,1,a']$. This number exists, since $F(a) \geq G(a)$. Suppose that $a' < b$. Then

$$F(a'+1) < G(a'+1),$$

$$F(a'+1)G(a') < F(a')G(a'+1),$$

$$F(k) > 0 \qquad \textit{for } k \in (a',1,b),$$

$$F(b) \geq 0,$$

$$A(k) \leq B(k) \qquad \textit{for } k \in (a',1,b).$$

It follows from Lemma 2.4.2 (with $a = a'$) that $F(b) < G(b)$. This contradiction shows that $a' = b$, proving the lemma. □

CHAPTER 3

KRAVČUK POLYNOMIALS

In this chapter, a number of properties of Kravčuk polynomials are derived, which will be used in the subsequent chapters.

3.1. Definition of and relationships between Kravčuk polynomials

Henceforth, q *denotes a real number greater than* 1 *and* n *denotes a natural number.*

For any $k \in \mathbb{N} \cup \{-1\}$, the *Kravčuk polynomial* K_k (*of degree* k *and with parameters* q *and* n) is defined by

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

for all $v \in \mathbb{R}$. In particular, $K_k(0) = (q-1)^k \binom{n}{k}$.

A simple expression for the generating power series exists.

LEMMA 3.1.1. *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 at the right-hand side. □

From this expression, an alternative formula for $K_k(v)$ follows.

LEMMA 3.1.2. *Let* $k \in \mathbb{N}$ *and* $v \in \mathbb{R}$. *Then*

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

PROOF.

$$\sum_{k=0}^{\infty} K_k(v)X^k = (1-X+qX)^{n-v}(1-X)^v =$$

$$= \sum_{j=0}^{\infty} \binom{n-v}{j}(1-X)^{n-j}(qX)^j = \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} \binom{n-v}{j}\binom{n-j}{i}(-X)^i(qX)^j =$$

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

Lemma 3.1.2 shows that K_k is indeed a polynomial of degree k. The following lemma proves a recurrence relation for Kravčuk polynomials.

LEMMA 3.1.3. *Let* $k \in \mathbb{N}$ *and* $v \in \mathbb{R}$. *Then*

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

PROOF. Differentiate the identity

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

to X, and multiply the result by $(1+(q-1)X)(1-X)$. One obtains

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

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

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

Comparing the coefficients of X^k, one finds

$$(k+1)K_{k+1}(v) + (q-2)kK_k(v) - (q-1)(k-1K_{k-1}(v) =$$

$$= ((q-1)n-qv)K_k(v) - (q-1)nK_{k-1}(v),$$

from which the lemma follows at once. $\square$

From this recurrence relation, it can be deduced that the zeros of successive Kravčuk polynomials are interlaced.

LEMMA 3.1.4. *Let* $k \in [0,1,n)$. *Then* K_k *has* k *distinct zeros in the interval* $(0,n)$. *Denoting these zeros in increasing order by* $v_1, v_2, \ldots, v_k$, *and the zeros of* K_{k-1} *by* $u_1, u_2, \ldots, u_{k-1}$, *then*

$$v_i < u_i < v_{i+1} \text{ for } i \in [1,1,k).$$

PROOF. First, it is observed that

$$\operatorname{sgn} K_k(0) = \operatorname{sgn} ((q-1)^k \binom{n}{k}) = 1$$

and

$$\operatorname{sgn} K_k(n) = \operatorname{sgn} ((-1)^k \binom{n}{k}) = (-1)^k,$$

provided $k \in [0,1,n]$.

The assertion of the lemma is trivial for $k = 0$, since $K_0 = 1$. Suppose it has been proved for certain k. Then

$$\operatorname{sgn} K_{k-1}(v_1) = \operatorname{sgn} K_{k-1}(0) = 1,$$

and

$$\operatorname{sgn} K_{k-1}(v_{i+1}) = -\operatorname{sgn} K_{k-1}(v_i) \qquad \text{for } i \in (0,1,k),$$

so

$$\operatorname{sgn} K_{k-1}(v_i) = -(-1)^i \qquad \text{for } i \in (0,1,k].$$

Since $K_k(v_i) = 0$, Lemma 3.1.4 yields

$$(k+1)K_{k+1}(v_i) = -(q-1)(n-k+1)K_{k-1}(v_i),$$

so

$$\operatorname{sgn} K_{k+1}(v_i) = -\operatorname{sgn} K_{k-1}(v_i) = (-1)^i \text{ for } i \in (0,1,k].$$

Therefore, K_{k+1} has zeros in the intervals $(0,v_1)$, (v_i,v_{i+1}) for $i \in (0,1,k)$, and (v_k,n). Since K_{k+1} is a nonzero polynomial of degree k+1, this proves

that K_{k+1} has exactly k+1 zeros in (0,n). Denoting these zeros in increasing order by $w_1, w_2, \ldots, w_{k+1}$, one has $w_1 < v_1$, $v_i < w_{i+1} < v_{i+1}$ for $i \in (0,1,k)$, and $v_k < w_{k+1}$. Therefore,

$$w_i < v_i < w_{i+1} \qquad \text{for } i \in (0,1,k+1),$$

proving the lemma by induction. □

The following lemma proves that Kravčuk polynomials are in a way self-dual.

LEMMA 3.1.5. *Let* $k \in \mathbb{N}$ *and* $\ell \in \mathbb{N}$. *Then*

$$\sum_{i=0}^{n} K_k(i)K_i(\ell) = \delta_{k,\ell} q^n.$$

PROOF. From Lemma 3.1.1 one derives

$$\sum_{k=0}^{\infty} \sum_{i=0}^{n} K_k(i)K_i(\ell)X^k = \sum_{i=0}^{n} K_i(\ell)(1+(q-1)X)^{n-i}(1-X)^i =$$

$$= (1+(q-1)X)^n \sum_{i=0}^{\infty} K_i(\ell)\left(\frac{1-X}{1+(q-1)X}\right)^i =$$

$$= (1+(q-1)X)^n \left(\frac{q}{1+(q-1)X}\right)^{n-\ell} \left(\frac{qX}{1+(q-1)X}\right)^{\ell} = q^n X^{\ell}.$$

Note that the second transition is permitted because of the integrality of ℓ. Otherwise, $K_i(\ell)$ does not vanish for $i > n$. □

From Lemma 3.1.5 the following inversion formula follows by straightforward verification.

LEMMA 3.1.6. *Let* $(\alpha_k)_{k=0}^n$ *and* $(\beta_i)_{i=0}^n$ *be two real sequences. Then*

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \quad \textit{for all } i \in [0,1,n]$$

if and only if

$$q^n \alpha_k = \sum_{i=0}^{n} \beta_i K_i(k) \quad \textit{for all } k \in [0,1,n].$$

Finally, a combined difference-recurrence relation for Kravčuk polynomials is established.

LEMMA 3.1.7. *Let* $k \in \mathbb{N}$ *and* $v \in \mathbb{R}$. *Then*

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

PROOF. From Lemma 3.1.1 one derives

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

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

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

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

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

3.2. The Lloyd polynomial

Henceforth, t *denotes a natural number smaller than or equal to* n.

The *Lloyd polynomial* $\Psi^{(n)}$ (*of degree* t *and with parameters* q *and* n) is defined by

$$\Psi^{(n)} = \sum_{k=0}^{t} K_k.$$

Obviously, $\Psi^{(n)}$ is a polynomial of degree t. The following identity holds.

LEMMA 3.2.1. *Let* $v \in \mathbb{R}$. *Then*

$$\Psi^{(n+1)}(v) = K_t(v-1).$$

PROOF. By Lemma 3.1.2 one has

$$\Psi^{(n)}(v) = \sum_{k=0}^{t} K_k(v) = \sum_{k=0}^{t} \sum_{j=0}^{k} (-1)^{k-j} q^j \binom{n-j}{k-j} \binom{n-v}{j} =$$

$$= \sum_{j=0}^{t} q^j \binom{n-v}{j} \sum_{k=j}^{t} (-1)^{k-j} \binom{n-j}{k-j} =$$

$$= \sum_{j=0}^{t} q^j \binom{n-v}{j} (-1)^{t-j} \binom{n-j-1}{t-j},$$

due to the well known identity $\sum_{i=0}^{k} (-1)^i \binom{n}{i} = (-1)^k \binom{n-1}{k}$. Hence

$$\psi^{(n+1)}(v) = \sum_{j=0}^{t} (-1)^{t-j} q^j \binom{n-j}{t-j} \binom{n-v+1}{j} = K_t(v-1). \quad \square$$

3.3. Properties of a Kravčuk polynomial

The values of the Kravčuk polynomial K_t^v are interrelated by a difference equation.

LEMMA 3.3.1. *Let* $v \in \mathbb{R}$. *Then*

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

PROOF. From Lemma 3.1.1 one derives

$$\sum_{k=0}^{\infty} ((q-1)(n-v)K_k(v+1) - (v+(q-1)(n-v)-qk)K_k(v) + vK_k(v-1))X^k =$$

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

$$+ qX\frac{d}{dX}((1+(q-1)X)^{n-v}(1-X)^v) + v(1+(q-1)X)^{n-v+1}(1-X)^{v-1} =$$

$$= (1+(q-1)X)^{n-v-1}(1-X)^{v-1}((q-1)(n-v)(1-X)^2 - (v+(q-1)(n-v))(1+(q-1)X)(1-X) +$$

$$+ qX((q-1)(n-v)(1-X) - v(1+(q-1)X)) + v(1+(q-1)X)^2) = 0. \quad \square$$

As a consequence of the above lemma, reference is made to the first (very weak) result concerning the zeros of K_t.

LEMMA 3.3.2. K_t *does not have two zeros which differ exactly by* 1.

PROOF. Suppose that $K_t(v_0) = K_t(v_0+1) = 0$ for some $v_0 \in \mathbb{R}$. Then from the difference equations follows that either $K_t(v) = 0$ for infinitely many $v \in \mathbb{R}$, or - if $v_0 \in [0,1,n-1]$ - $K_t(v) = 0$ for $v \in [0,1,n]$. Hence, K_t has at least n+1 zeros, which is impossible for a nonzero polynomial of degree $t \leq n$. $\square$

Next, the difference equation is transformed according to the methods developed in Section 2.4. Define the function M by

$$M(v) = \frac{(q-1)^{\frac{1}{2}v} K_t(v)}{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}$$

for all $v \in (-1,n+1)$.

LEMMA 3.3.3. *Let* $v \in (0,n)$. *Then*

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

PROOF. By Lemma 3.3.1 and the definition of M one has

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

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

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

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. □

It is easier to work with $(q-1)n/q-v$ than with v. Therefore, define x by

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

and the functions N and C by

$$N(x) = M(v),$$

and

$$C(x) = \frac{v+(q-1)(n-v)-qt}{2(q-1)^{\frac{1}{2}}} \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!}$$

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

LEMMA 3.3.4. *Let* $v \in (0,n)$. *Then*

$$N(x+1) - C(x)N(x) + N(x-1) = 0.$$

CHAPTER 4

PERFECT CODES AND KRAVČUK POLYNOMIALS

This chapter contains a number of known results appertaining to perfect codes, which will be used in the subsequent chapters. A short proof of Lloyd's theorem will be presented. The proof is based on the linear programming bound, which will also be derived.

First, some basic concepts concerning block codes will be surveyed. For a thorough treatment of the subject, the reader is referred to MACWILLIAMS & SLOANE [20].

4.1. Basic concepts concerning codes

In the previous chapter, q was permitted to be a real number greater than 1. *Henceforth, it is assumed that* q *is a natural number satisfying* $q \geq 2$.

Let Q be a set of q elements including a zero element 0. Q will be called the *alphabet*.

A *word* (of *length* n *over* Q) is a sequence of n elements of Q.

The word $(0)_{i=1}^{n}$ is called the *origin* 0.

The (*Hamming*) *distance* $d_H(x,y)$ between two words x and y is the number of positions by which they differ: if $x = (x_i)_{i=1}^{n}$ and $y = (y_i)_{i=1}^{n}$, then

$$d_H(x,y) = |\{i | i \in (0,1,n] \wedge x_i \neq y_i\}|.$$

The (*Hamming*) *weight* $|x|$ of a word x is the distance between x and the origin:

$$|x| = d_H(x,0).$$

With this distance function, the set $X = Q^n$ of all words becomes a metric space.

A (q-*ary*) *code* (of *length* n) is a subset of X. A 2-ary code is called *binary*.

An element of the code is called a *codeword*.

A code consisting of at most one codeword is called *degenerate*.

The code X is called *trivial*.

A code is called t-*error correcting* if the (closed, solid) spheres of radius t around the codewords in the metric space X are disjoint.

If the spheres form a partitioning of X, the code is called t-*perfect*. A *perfect* code is a code that is t-perfect for some $t \in \mathbb{N}$.

The *distance distribution* of a nonempty code C is the sequence $(A_i)_{i=0}^n$, where A_i equals the average number of codewords at distance i from a fixed codeword, i.e.

$$A_i = |C|^{-1} \sum_{x \in C} |\{y | y \in C \wedge d_H(x,y) = i\}| =$$

$$= |C|^{-1} |\{(x,y) | x \in C \wedge y \in C \wedge d_H(x,y) = i\}|.$$

Notice that $A_0 = 1$.

Finally, the *dual distance distribution* of C is the sequence $(B_k)_{k=0}^n$, where

$$B_k = \sum_{i=0}^{n} A_i K_k(i),$$

K_k being the Kravčuk polynomial of degree k. The use of this last definition will become clear in the next section. Notice that $B_0 = |C|$.

4.2. The linear programming bound

In this section, the linear programming bound for error correcting codes is derived by elementary means.

Suppose, without loss of generality, that $Q = [0,1,q)$, and define the inner product $\langle x,y \rangle$ of two words $x = (x_i)_{i=1}^n$ and $y = (y_i)_{i=1}^n$ by

$$\langle x,y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Furthermore, let ω be some primitive complex q-th root of unity. A remarkable relation between the "Hamming scheme" and Kravčuk polynomials can now be established.

LEMMA 4.2.1. *Let* i *and* k *be natural numbers, and let* x *be a word in* $X = Q^n$ *of weight* i. *Then*

$$\sum_{\substack{z\in X\\ |z|=k}} \omega^{<x,z>} = K_k(i).$$

PROOF. Without loss of generality it can be assumed that

$$x = (x_1,x_2,\ldots,x_i,0,0,\ldots,0),$$

with $x_h \neq 0$ for $h \in (0,1,i]$.

Furthermore, let $j \in [0,1,k]$, and let $h_1,h_2,\ldots,h_k$ be integers such that

$$0 < h_1 < h_2 <\ldots< h_j \leq i < h_{j+1} < h_{j+2} <\ldots< h_k \leq n,$$

and let D be the set of all words (of weight k) which have their nonzero coordinates precisely in the positions $h_1,h_2,\ldots,h_k$. Then

$$\sum_{z\in D} \omega^{<x,z>} = \sum_{z_{h_1},\ldots,z_{h_k}\in Q\setminus\{0\}} \omega^{x_{h_1}z_{h_1}+\ldots+x_{h_j}z_{h_j}} =$$

$$= (q-1)^{k-j} \prod_{m=1}^{j} \sum_{z\in Q\setminus\{0\}} \omega^{x_{h_m}z} = (-1)^j(q-1)^{k-j}.$$

Hence,

$$\sum_{\substack{z\in X\\ |z|=k}} \omega^{<x,z>} = \sum_{j=0}^{k} \binom{i}{j}\binom{n-i}{k-j}(-1)^j(q-1)^{k-j} = K_k(i). \quad \square$$

From Lemma 4.2.1 it follows that the dual distance distribution of a code is weakly positive.

LEMMA 4.2.2. *Let* $(B_k)_{k=0}^n$ *be the dual distance distribution of a nonempty code. Then* $B_k \geq 0$ *for* $k \in [0,1,n]$.

PROOF. Let $(A_i)_{i=0}^n$ be the distance distribution of the code, and let M be its cardinality. Then

$$MB_k = M \sum_{i=0}^{n} A_i K_i(i) = \sum_{i=0}^{n} \sum_{\substack{x,y\in C \\ d_H(x,y)=i}} \sum_{\substack{z\in X \\ |z|=k}} \omega^{<x-y,z>} =$$

$$= \sum_{\substack{z\in X \\ |z|=k}} \Big| \sum_{x\in C} \omega^{<x,z>} \Big|^2 \geq 0.$$

[Here x-y denotes the coordinatewise difference modulo q of x and y.] □

The above lemma provides a powerful tool in deriving upper bounds for the maximum cardinality of a code of fixed length and minimum distance. In each particular case the maximum is found by solving a linear programming problem. This explains the name "linear programming bound". A survey of applications can be found in BEST [3].

Sometimes it is easier to switch to the dual LP-problem: any solution of the latter furnishes an upper bound for the optimal solution of the primal problem. The next lemma investigates when this bound is tight.

LEMMA 4.2.3. *Let* $(A_i)_{i=0}^n$ *and* $(B_k)_{k=0}^n$ *be respectively the distance distribution and the dual distance distribution of a code* C. *Furthermore, let* $(\alpha_k)_{k=0}^n$ *and* $(\beta_i)_{i=0}^n$ *be two sequences of real numbers such that*

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \qquad \textit{for} \quad i \in [0,1,n],$$

$$\alpha_k \geq 0 \qquad \textit{for} \quad k \in [1,1,n],$$

$$\beta_i \leq 0 \ \textit{if} \ A_i > 0 \qquad \textit{for} \quad i \in [1,1,n].$$

Then

$$\alpha_0|C| = \beta_0$$

if and only if

$$\alpha_j B_j = \beta_j A_j = 0 \qquad \textit{for} \quad j \in [1,1,n].$$

PROOF. Since

$$\alpha_0|C| = \alpha_0 B_0 \le \sum_{k=0}^{n} \alpha_k B_k = \sum_{k=0}^{n} \sum_{i=0}^{n} \alpha_k K_k(i) A_i = \sum_{i=0}^{n} \beta_i A_i \le$$

$$\le \beta_0 A_0 = \beta_0,$$

$\alpha_0|C| = \beta_0$ holds if and only if $\sum_{k=1}^{n} \alpha_k B_k = \sum_{i=1}^{n} \beta_i A_i = 0$. □

As an application of the above lemma, an inequality is derived which was discovered by F.J. MACWILLIAMS [19] for linear codes, and later generalized by P. DELSARTE [5] to general codes.

LEMMA 4.2.4. (MacWilliams inequality.) *Let* C *be a nonempty* t*-error correcting code with dual distance distribution* $(B_k)_{k=0}^{n}$, *where* $t < n$. *Then there are at least* t *nonzero dual distances:*

$$|\{k|k \in [1,1,n] \wedge B_k \neq 0\}| \ge t.$$

PROOF. Suppose that $|\{k|k \in [1,1,n] \wedge B_k \neq 0\}| < t$. Then a nonzero polynomial γ of degree less than t exists such that $\gamma(k) = 0$ if $k \in [1,1,n]$ and $B_k \neq 0$. Define

$$\alpha_k = k\gamma^2(k) \qquad \text{for } k \in [0,1,n],$$

and

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \qquad \text{for } i \in [0,1,n].$$

Then, by Lemma 3.1.6,

$$\sum_{i=0}^{n} \beta_i K_i(k) = q^n \alpha_k.$$

Since α_k is a polynomial of degree less than 2t in k, and $K_i(k)$ is a polynomial of degree i in k, it follows that $\beta_i = 0$ if $i \in [2t,1,n]$.

Let $(A_i)_{i=0}^{n}$ denote the distance distribution of C. Then $A_i = 0$ if $i \in [1,1,2t]$. Thus $\alpha_j B_j = \beta_j A_j = 0$ for $j \in [1,1,n]$. Hence Lemma 4.2.3 yields

$$0 = \alpha_0|C| = \beta_0 = \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} \binom{n}{k} (q-1)^k \, k \, \gamma^2(k).$$

But this implies that $\gamma(k) = 0$ for $k \in [1,1,n]$, so γ vanishes identically. This contradiction proves the lemma. □

REMARK. The number of nonzero dual distances is called the "external distance" of the code. The lemma remains valid if the code is t-error detecting only.

4.3. Lloyd's theorem

Lloyd's theorem states a strong necessary condition which should be fulfilled in order that a code may be perfect. The theorem was first proved by S.P. LLOYD [18] for binary linear codes, and later generalized by F.J. MACWILLIAMS [19] to general linear codes; finally P. DELSARTE [5] and H.W. LENSTRA Jr. [10] proved (independently) the general theorem for arbitrary codes. Remind that $\Psi^{(n)}$ was defined in Section 3.2.

LEMMA 4.3.1. (Lloyd's theorem) *Let* C *be a* t*-perfect code of length* $n \geq t$. *Then the Lloyd polynomial* $\Psi^{(n)}$ *has* t *distinct zeros in* $[1,1,n]$.

PROOF. Define

$$\alpha_k = (\Psi^{(n)}(k))^2 \qquad \text{for } k \in [0,1,n],$$

and

$$\beta_i = \sum_{k=0}^{n} \alpha_k K_k(i) \qquad \text{for } i \in [0,1,n].$$

Then, as in the proof of Lemma 4.2.4, one finds

$$\sum_{i=0}^{n} \beta_i K_i(k) = q^n \alpha_k,$$

so $\beta_i = 0$ if $i > 2t$. Furthermore, by the definition of $\Psi^{(n)}$,

$$\beta_0 = \sum_{k=0}^{n} \alpha_k K_k(0) = \sum_{k=0}^{n} (q-1)^k \binom{n}{k} \Big(\sum_{j=0}^{t} K_j(k) \Big)^2 =$$

$$= \sum_{j,j'=0}^{t} \sum_{k=0}^{n} (q-1)^k \binom{n}{k} K_j(k) K_{j'}(k) = q^n \sum_{j,j'=0}^{t} \delta_{j,j'} \binom{n}{j} (q-1)^j =$$

$$= q^n \sum_{j=0}^{t} \binom{n}{j} (q-1)^j,$$

and

$$\alpha_0 = (\Psi^{(n)}(0))^2 = (\sum_{j=0}^{t} \binom{n}{j}(q-1)^j)^2.$$

Since C is t-perfect, one has

$$|C| = q^n / \sum_{j=0}^{t} \binom{n}{j}(q-1)^j.$$

Hence

$$\alpha_0 |C| = \beta_0.$$

Lemma 4.2.3 proves that $\alpha_k B_k = 0$ for $k \in [1,1,n]$. Subsequently, Lemma 4.2.4 proves that there are at least t nonzero dual distances. Hence there are at least t values of k for which $\alpha_k = 0$, so $\Psi^{(n)}(k) = 0$ for at least t values of k. This proves the lemma. □

4.4. Known results about perfect codes

Not a single nondegenerate, nonbinary perfect code correcting at least three errors is known. For binary codes, the following result was established by A. TIETÄVÄINEN and A. PERKO.

LEMMA 4.4.1. *The only nondegenerate perfect binary codes correcting at least three errors are the* 3*-perfect Golay code of length* 23 *and the* t*-perfect repetition codes of length* 2t+1 *(for any* $t \geq 3$*).*

Proof can be found in TIETÄVÄINEN & PERKO [30] or in VAN LINT [16]. The uniqueness of the binary Golay code was proved by S.L. SNOVER [24].

In the course of time, several nonexistence proofs for classes of nonbinary perfect codes have been presented. The following results are due to H.F.H. REUVERS [22] and H. LAAKSO [9] respectively.

LEMMA 4.4.2. *Let* $t \in \{3,4,5\}$*, and* $q \geq 3$*. Then there are no nondegenerate* t*-perfect* q*-ary codes.*

LEMMA 4.4.3. *Let* $t \geq 3$*,* $q \geq 3$*, and let* q *have at most three distinct prime divisors. Then there are no nondegenerate* t*-perfect* q*-ary codes.*

CHAPTER 5

LONG-WAVE KRAVČUK POLYNOMIALS

5.1. Scope

In the previous chapters, t was permitted to be a natural number less than or equal to n. *Henceforth it is assumed in addition that* $t \geq 7$ *but* $t \neq 8$.

In this and the next two chapters, Kravčuk polynomials of relatively large parameter n (compared to q and t) are considered. These polynomials oscillate relatively slowly, explaining the title of this chapter. In Chapter 8 the "short-wave polynomials" will be investigated.

To make the distinction more precise, the variable ω is introduced according to

$$\omega = q\left(\frac{2t+1}{2(q-1)n}\right)^{\frac{1}{2}}.$$

The number ω will reveal itself as having connections with the "wave-number" of the Kravčuk polynomial K_t in the region of interest.

In Chapters 5,6 and 7, it will be assumed that $\omega \leq 1/(2t)$.

In terms of n, this means that

$$n \geq \frac{2q^2t^2(2t+1)}{q-1}.$$

In the present chapter, the weaker assumption $n \geq 2qt^3$ suffices. It becomes apparent that under this assumption Kravčuk polynomials of odd degree are almost antisymmetric with respect to $(q-1)n/q$, while Kravčuk polynomials of even degree are almost symmetric with respect to this number. This most informal statement lacks any mathematical significance, but it is the crucial observation which is the basis of the entire thesis. In particular, the adverb "almost" will enable us to prove that the three or four zeros closest to $(q-1)n/q$ can never be integral simultaneously.

For this purpose, some results concerning Kravčuk polynomials in a neighbourhood of $\nu = (q-1)n/q$ will be established in this chapter.

5.2. An estimate for K_k at $(q-1)n/q$

In this section a rapidly converging expansion for $K_k(\nu)$, where $\nu = (q-1)n/q$, will be deduced. In order to simplify notation, for each $k \in \mathbb{N}$ the function L_k is introduced by defining

$$L_k(x) = (-1)^{\lceil \frac{1}{2}k \rceil} K_k(\nu - x).$$

(The sign has been chosen in such a way that $L_k(0)$ is positive; cf. Lemma 5.2.5.) Furthermore, for each $k \in \mathbb{N}$ and $c \in \mathbb{N} \cup \{-1\}$, the number $a_{k,c}$ is defined by

$$a_{k,c} = \binom{n/q}{c} \sum_{\substack{j_1,\ldots,j_c \geq 1 \\ j_1+\ldots+j_c=k}} \prod_{i=1}^{c} ((j_i-1)\binom{q}{j_i}).$$

LEMMA 5.2.1. *Let* $k \in \mathbb{N}$. *Then*

$$L_k(0) = (-1)^{\lfloor \frac{1}{2}k \rfloor} \sum_{c=0}^{\lfloor \frac{1}{2}k \rfloor} (-1)^c a_{k,c}.$$

PROOF. By Lemma 3.1.1 one has

$$\sum_{k=0}^{\infty} (-1)^{\lceil \frac{1}{2}k \rceil} L_k(0) X^k = (1+(q-1)X)^{n/q}(1-X)^{(q-1)n/q} =$$

$$= ((1+(q-1)X)(1-X)^{q-1})^{n/q} = ((1-X)^q + qX(1-X)^{q-1})^{n/q} =$$

$$= (\sum_{j=0}^{\infty} \binom{q}{j}(-X)^j + qX \sum_{j=0}^{\infty} \binom{q-1}{j}(-X)^j)^{n/q} =$$

$$= (\sum_{j=0}^{\infty} (\binom{q}{j} - q\binom{q-1}{j-1})(-X)^j)^{n/q} = (1 - \sum_{j=1}^{\infty} (j-1)\binom{q}{j}(-X)^j)^{n/q} =$$

$$= \sum_{c=0}^{\infty} \binom{n/q}{c} (-\sum_{j=1}^{\infty} (j-1)\binom{q}{j}(-X)^j)^c =$$

$$= \sum_{c=0}^{\infty} (-1)^c \binom{n/q}{c} \sum_{j_1,\ldots,j_c \geq 1} \prod_{i=1}^{c} ((j_i-1)\binom{q}{j_i}(-X)^{j_i}) =$$

$$= \sum_{k=0}^{\infty} (-X)^k \sum_{c=0}^{\infty} (-1)^c a_{k,c}.$$

Comparison of corresponding coefficients gives the required expression for $L_k(0)$. Note that $a_{k,c} = 0$ if $c > \frac{1}{2}k$. □

Concerning the numbers $a_{k,c}$, several identities are of importance.

LEMMA 5.2.2. *Let* $c \in \mathbb{N}$. *Then*

$$a_{2c,c} = \binom{n/q}{c}\binom{q}{2}^c,$$

$$a_{2c+1,c} = 2\binom{n/q}{c}\binom{q}{2}^{c-1}\binom{q}{3}c,$$

$$a_{2c+2,c} = \binom{n/q}{c}\binom{q}{2}^c(q-2)c\left(\frac{1}{4}(q-3)+\frac{2}{9}(q-2)(c-1)\right),$$

$$a_{2c+3,c} = \binom{n/q}{c}\binom{q}{2}^{c-1}\binom{q}{3}c\left(\frac{1}{5}(q-3)(q-4)+\frac{1}{2}(q-2)(q-3)(c-1)+\right.$$

$$\left.+\frac{4}{27}(q-2)^2(c-1)(c-2)\right).$$

PROOF.

$$a_{2c,c} = \binom{n/q}{c} \sum_{\substack{j_1,\ldots,j_c\geq 2\\ j_1+\ldots+j_c=2c}} \prod_{i=1}^{c}\left((j_i-1)\binom{q}{j_i}\right) = \binom{n/q}{c}\binom{q}{2}^c;$$

$$a_{2c+1,c} = \binom{n/q}{c} \sum_{\substack{j_1,\ldots,j_c\geq 2\\ j_1+\ldots+j_c=2c+1}} \prod_{i=1}^{c}\left((j_i-1)\binom{q}{j_i}\right) = \binom{n/q}{c}c\binom{q}{2}^{c-1}2\binom{q}{3};$$

$$a_{2c+2,c} = \binom{n/q}{c} \sum_{\substack{j_1,\ldots,j_c\geq 2\\ j_1+\ldots+j_c=2c+2}} \prod_{i=1}^{c}\left((j_i-1)\binom{q}{j_i}\right) =$$

$$= \binom{n/q}{c}\left(c\binom{q}{2}^{c-1}3\binom{q}{4}+\binom{c}{2}\binom{q}{2}^{c-2}4\binom{q}{3}^2\right);$$

$$a_{2c+3,c} = \binom{n/q}{c} \sum_{\substack{j_1,\ldots,j_c\geq 2\\ j_1+\ldots+j_c=2c+3}} \prod_{i=1}^{c}\left((j_i-1)\binom{q}{j_i}\right) =$$

$$= \binom{n/q}{c}\left(c\binom{q}{2}^{c-1}4\binom{q}{5}+c(c-1)\binom{q}{2}^{c-2}2\binom{q}{3}3\binom{q}{4}+\binom{c}{3}\binom{q}{2}^{c-3}8\binom{q}{3}^3\right).$$ □

From these identities, some inequalities can be derived.

LEMMA 5.2.3. *Let* $k \in \mathbb{N}$, $k \geq 2$, $n \geq 2qk^3$. *Then*

$$a_{k,\lfloor \frac{1}{2}k\rfloor -1} \le \frac{q-2}{36q}\, a_{k,\lfloor \frac{1}{2}k\rfloor}$$

and

$$a_{k-2,\lfloor \frac{1}{2}k\rfloor -1} \le \frac{2}{3q(q-1)k^2}\, a_{k,\lfloor \frac{1}{2}k\rfloor}.$$

PROOF. Put $\ell = \lfloor \frac{1}{2}k\rfloor$. Then $n/q-\ell+1 \ge 2k^3-\frac{1}{2}k \ge 2k(k^2-1) \ge 4\ell(4\ell^2-1)$. Hence

$$a_{2\ell,\ell-1} = \binom{n/q}{\ell-1}\binom{q}{2}^{\ell-1}(q-2)(\ell-1)\left(\tfrac{1}{4}(q-3)+\tfrac{2}{9}(q-2)(\ell-2)\right) \le$$

$$\le \binom{n/q}{\ell}\binom{q}{2}^{\ell}\frac{2(q-2)\ell(\ell-1)}{q(q-1)(n/q-\ell+1)}\cdot\frac{2}{9}(q-2)\ell \le \frac{q-2}{36q}\, a_{2\ell,\ell};$$

$$a_{2\ell+1,\ell-1} =$$

$$= \binom{n/q}{\ell-1}\binom{q}{2}^{\ell-2}\binom{q}{3}(\ell-1)\left(\tfrac{1}{5}(q-3)(q-4)+\tfrac{1}{2}(q-2)(q-3)(\ell-2)+\right.$$

$$\left.+\tfrac{4}{27}(q-2)^2(\ell-2)(\ell-3)\right) \le$$

$$\le 2\binom{n/q}{\ell}\binom{q}{2}^{\ell-1}\binom{q}{3}\ell\frac{\ell-1}{q(q-1)(n/q-\ell+1)}\cdot\frac{4}{27}(q-2)^2\ell^2 \le \frac{q-2}{36q}\, a_{2\ell+1,\ell};$$

$$a_{2\ell-2,\ell-1} \le \binom{n/q}{\ell-1}\binom{q}{2}^{\ell-1} = \binom{n/q}{\ell}\binom{q}{2}^{\ell}\frac{2\ell}{q(q-1)(n/q-\ell+1)} \le$$

$$\le \frac{2}{3q(q-1)k^2}\, a_{2\ell,\ell};$$

$$a_{2\ell-1,\ell-1} = 2\binom{n/q}{\ell-1}\binom{q}{2}^{\ell-2}\binom{q}{3}(\ell-1) =$$

$$= 2\binom{n/q}{\ell}\binom{q}{2}^{\ell-1}\binom{q}{3}\ell\frac{2(\ell-1)}{q(q-1)(n/q-\ell+1)} \le \frac{2}{3q(q-1)k^2}\, a_{2\ell+1,\ell}.$$

These inequalities prove the lemma. □

LEMMA 5.2.4. *Let* $k \in \mathbb{N}$ *and* $n \ge 2qk^3$. *Then* $(a_{k,c})_{c=0}^{\lfloor \frac{1}{2}k\rfloor}$ *is monotonically increasing.*

PROOF. The sequence $(\beta_j)_{j=0}^{\infty}$ defined by $\beta_j = \max(0,(j-1)\binom{q}{j})$ is logconcave, since it is the product of the logconcave sequences $(\max(0,j-1))_{j=0}^{\infty}$ and $(\binom{q}{j})_{j=0}^{\infty}$ (Lemma 2.3.3). Hence, by Lemma 2.3.5, the sequence $(b_{k,c})_{c=0}^{\infty}$ defined by

$$b_{k,c} = \sum_{\substack{j_1,\ldots,j_c \geq 1 \\ j_1+\ldots+j_c=k}} \prod_{i=1}^{c} ((j_i-1)\binom{q}{j_i})$$

is logconcave. Since finally the sequence $(\binom{n/q}{c})_{c=0}^{\lfloor \frac{1}{2}k \rfloor}$ is logconcave (notice that $\lfloor \frac{1}{2}k \rfloor \leq n/q$), and $a_{k,c} = \binom{n/q}{c} b_{k,c}$, it follows that the sequence $(a_{k,c})_{c=0}^{\lfloor \frac{1}{2}k \rfloor}$ is logconcave. Together with $a_{k,\lfloor \frac{1}{2}k \rfloor - 1} \leq a_{k,\lfloor \frac{1}{2}k \rfloor}$ if $k \geq 2$ (Lemma (5.2.3), this yields the assertion of the lemma. □

The Lemmas 5.2.1 and 5.2.4 combine into the following result.

LEMMA 5.2.5. *Let* $k \in \mathbb{N}$ *and* $n \geq 2qk^3$. *Then*

$$0 \leq a_{k,\lfloor \frac{1}{2}k \rfloor} - a_{k,\lfloor \frac{1}{2}k \rfloor - 1} \leq L_k(0) \leq a_{k,\lfloor \frac{1}{2}k \rfloor}.$$

5.3. An estimate for K_k in a neighbourhood of $(q-1)n/q$

In this section, the results of the previous section are extended to an estimate for L_k in a neighbourhood of 0. For that purpose, define the functions λ_j for $j \in \mathbb{N}$ by

$$\sum_{j=0}^{\infty} \lambda_j(x) X^j = (1+(q-1)X)^x (1-X)^{-x}.$$

LEMMA 5.3.1. *Let* $k \in \mathbb{N}$ *and* $x \in \mathbb{R}$. *Then*

$$L_k(x) = (-1)^{\lceil \frac{1}{2}k \rceil} \sum_{j=0}^{k} (-1)^{\lceil \frac{1}{2}j \rceil} \lambda_{k-j}(x) L_j(0).$$

PROOF. By Lemma 3.1.1 one has

$$\sum_{k=0}^{\infty} (-1)^{\lceil \frac{1}{2}k \rceil} L_k(x) X^k = (1+(q-1)X)^{n/q+x} (1-X)^{(q-1)n/q-x} =$$

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

$$= \Big(\sum_{j=0}^{\infty} \lambda_j(x) X^j\Big)\Big(\sum_{j=0}^{\infty} (-1)^{\lceil \frac{1}{2}j \rceil} L_j(0) X^j\Big).$$

This proves the lemma. □

Concerning the functions λ_k, several identities and inequalities will be needed.

LEMMA 5.3.2. *Let* $x \in \mathbb{N}$ *and* $k \in \mathbb{N}$. *Then*

$$\lambda_k(x) = \sum_{j=0}^{k} \binom{k-1}{k-j}\binom{x}{j} q^j \geq 0,$$

$$\lambda_0(x) = 1,$$

$$\lambda_1(x) = qx,$$

$$\lambda_2(x) = qx(\tfrac{1}{2}q(x-1)+1) \leq \tfrac{1}{2}q^2x^2,$$

$$\lambda_3(x) = qx(\tfrac{1}{6}q^2x^2 - \tfrac{1}{2}q^2x + \tfrac{1}{3}q^2 + qx - q + 1) \leq \tfrac{1}{4}q^3x^3,$$

$$\lambda_{k+2}(x) \leq \tfrac{1}{2}q^2x^2\lambda_k(x).$$

PROOF. By the definition of λ_k, it is known that

$$\sum_{k=0}^{\infty} \lambda_k(x)X^k = (1-X+qX)^x(1-X)^{-x} = \sum_{j=0}^{\infty} \binom{x}{j}(qX)^j(1-X)^{-j} =$$
$$= \sum_{j=0}^{\infty} \binom{x}{j}(qX)^j \sum_{i=0}^{\infty} \binom{-j}{i}(-X)^i = \sum_{j=0}^{\infty}\sum_{i=0}^{\infty} \binom{x}{j}\binom{i+j-1}{i} q^j X^{i+j} =$$
$$= \sum_{k=0}^{\infty} X^k \sum_{j=0}^{k} \binom{k-1}{k-j}\binom{x}{j} q^j.$$

Comparison of corresponding coefficients yields the expression for $\lambda_k(x)$. The identities and inequalities for $\lambda_0(x)$, $\lambda_1(x)$, $\lambda_2(x)$, and $\lambda_3(x)$ follow straightforwardly.

Furthermore, from the power series expansion

$$\sum_{k=0}^{\infty} \lambda_k(x)X^k = (1+(q-1)X)^x(1-X)^{-x},$$

it follows that the sequence $(\lambda_k(x))_{k=0}^{\infty}$ is logconcave (cf. Lemma 2.3.4). This proves the last inequality. □

Next, it will be proved that - under certain conditions - the expansion for $L_k(x)$ given in Lemma 5.3.1 can be decomposed into two alternating series in which terms increase monotonically in absolute value.

LEMMA 5.3.3. *Let* $j,k,x \in \mathbb{N}$, $2 \leq j \leq k$, $n \geq 2qk^3$, *and* $1 \leq x \leq k$. *Then*

$$0 \leq \lambda_{k-j+2}(x)L_{j-2}(0) \leq \lambda_{k-j}(x)L_j(0).$$

PROOF. By Lemmas 5.2.5 and 5.3.2, it suffices to prove that

$$\frac{1}{2}q^2x^2a_{j-2,\lfloor\frac{1}{2}j\rfloor-1} \le a_{j,\lfloor\frac{1}{2}j\rfloor} - a_{j,\lfloor\frac{1}{2}j\rfloor-1}.$$

By Lemma 5.2.3 it is known that

$$a_{j,\lfloor\frac{1}{2}j\rfloor-1} \le \frac{1}{36}\, a_{j,\lfloor\frac{1}{2}j\rfloor},$$

and also that

$$\frac{1}{2}q^2x^2a_{j-2,\lfloor\frac{1}{2}j\rfloor-1} \le \frac{q^2x^2}{3q(q-1)k^2}\, a_{j,\lfloor\frac{1}{2}j\rfloor} \le \frac{2}{3}\, a_{j,\lfloor\frac{1}{2}j\rfloor}.$$

This proves the lemma. □

Finally, an upper bound is established for $L_k(x)$ in the case of k being odd.

LEMMA 5.3.4. *Let* $\ell,x \in \mathbb{N}$, $x \le \ell$, *and* $n \ge 2q(2\ell+1)^3$. *Then*

$$L_{2\ell+1}(x) \le \frac{17}{72}q\, a_{2\ell,\ell}(3\ell-4x).$$

PROOF. By Lemma 5.3.1 one has

$$L_{2\ell+1}(x) = (-1)^{\ell+1}\Big(\sum_{j=0}^{2\ell+1}(-1)^{\lceil\frac{1}{2}j\rceil}\lambda_{2\ell-j+1}(x)L_j(0)\Big) =$$

$$= (-1)^{\ell}\Big(\sum_{i=0}^{\ell}(-1)^i\,\lambda_{2\ell-2i}(x)L_{2i+1}(0) - \sum_{i=0}^{\ell}(-1)^i\lambda_{2\ell-2i+1}(x)L_{2i}(0)\Big).$$

By Lemma 5.3.3, in both series on the right-hand side the terms alternate in sign, and increase in absolute value. Hence, from Lemmas 5.3.2, 5.2.5, 5.2.2, and 5.2.3 it follows (notice that $a_{2\ell,\ell} \ge 0$ because of $\ell \le n/q$) that

$$L_{2\ell+1}(x) \le \lambda_0(x)L_{2\ell+1}(0) - \lambda_1(x)L_{2\ell}(0) + \lambda_3(x)L_{2\ell-2}(0) \le$$

$$\le a_{2\ell+1,\ell} - qx(a_{2\ell,\ell}-a_{2\ell,\ell-1}) + \frac{1}{4}q^3x^3a_{2\ell-2,\ell-1} \le$$

$$\le a_{2\ell,\ell}\Big(\frac{2(q-2)\ell}{3} - qx\Big(1-\frac{q-2}{36q}\Big) + \frac{1}{4}q^3x^3\,\frac{1}{6q(q-1)\ell^2}\Big) \le$$

$$\leq a_{2\ell,\ell}\left(\frac{2}{3}(q-2)\ell - \frac{17}{18}\,qx + \frac{1}{24}\,(q+2)\ell\right) \leq$$

$$\leq \frac{17}{72}\,q a_{2\ell,\ell}(3\ell-4x). \quad \square$$

5.4. The central zeros

In this section, the results of the previous two sections are used to prove that any Kravčuk polynomial of odd degree has a zero very close to ν. For Kravčuk polynomials of even degree, a related result will be deduced. The results will be formulated in terms of the function N, defined in Section 3.3.

LEMMA 5.4.1. *If* t *is odd, then* L_t *has a zero in the interval* $[0,\frac{1}{2}(t-1)]$.

PROOF. By Lemma 5.2.5, $L_t(0) \geq 0$, while Lemma 5.3.4 yields that $L_t(\frac{1}{2}(t-1)) \leq 0$. $\square$

LEMMA 5.4.2. *Suppose that* t *is even. Then*

$$L_t(\tfrac{1}{2}t-1) \leq L_t(\tfrac{1}{2}t-2).$$

Moreover, L_t *has a zero in the interval* $[-1,\frac{1}{2}t-2]$ *or*

$$L_t(-1) \leq L_t(0).$$

PROOF. Lemma 3.1.7 is easily transformed in terms of L_t:

$$L_t(x+1) - L_t(x) = L_{t-1}(x+1) + (q-1)L_{t-1}(x).$$

Lemma 5.3.4 proves that both terms on the right-hand side are weakly negative for $x = \frac{1}{2}t-2$ (recall that $t \geq 10$). Hence

$$L_t(\tfrac{1}{2}t-1) \leq L_t(\tfrac{1}{2}t-2).$$

It is also known that $L_{t-1}(0) \geq 0$ by Lemma 5.2.5. Two possibilities are distinguished:

1. $L_{t-1}(-1) \geq 0$. Then $L_t(0) - L_t(-1) \geq 0$.
2. $L_{t-1}(-1) < 0$. Then L_{t-1} must have at least two zeros in the interval

$[-1,\frac{1}{2}t-2]$. Hence, by the interlacing property of the zeros of Kravčuk polynomials (Lemma 3.1.4), L_t must have a zero in that interval. □

The last two lemmas combine into the following result.

LEMMA 5.4.3. *At least one of the following two alternatives holds:*

1. L_t *has a zero in the interval* $[-1,\frac{1}{2}(t-1)]$;

2. $t \geq 10$, $L_t(-1) \leq L_t(0)$, *and* $L_t(\frac{1}{2}t-1) \leq L_t(\frac{1}{2}t-2)$.

If the second alternative holds, it is obvious that there is an $x_0 \in [-\frac{1}{2},\frac{1}{2}(t-3)]$ such that $L_t(x_0-\frac{1}{2}) = L_t(x_0+\frac{1}{2})$, which means that L_t behaves like an even function in a neighbourhood of x_0, in contrast to the first case, where L_t behaves more like an odd function. We shall need a related result concerning the function N rather than L_t.

LEMMA 5.4.4. *At least one of the following two alternatives holds:*

1. *there is an* $x_0 \in [-1,\frac{1}{2}(t-1)]$ *such that* $N(x_0) = 0$;

2. $t \geq 10$ *and there is an* $x_0 \in [-\frac{1}{2},\frac{1}{2}(t-3)]$ *such that* $N(x_0-\frac{1}{2}) = N(x_0+\frac{1}{2})$.

PROOF. From the definitions of N, M, and L_t it follows that

$$N(x) = M(v) = \frac{(q-1)^{\frac{1}{2}v}K_t(v)}{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!} = \frac{(-1)^{\lceil\frac{1}{2}t\rceil}(q-1)^{\frac{1}{2}v}L_t(x)}{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!},$$

where $v = (q-1)n/q-x$.

If the first alternative in Lemma 5.4.3 holds, x_0 is chosen such that $L_t(x_0) = 0$. This proves the lemma in this case.

Suppose that the second alternative holds. Due to $L_t(-1) \leq L_t(0)$ and Lemma 2.2.6 one has

$$(-1)^{\lceil\frac{1}{2}t\rceil}N(-1) = \frac{(q-1)^{\frac{1}{2}(q-1)n/q+\frac{1}{2}}L_t(-1)}{(\frac{1}{2}(q-1)n/q)!(\frac{1}{2}n/q-1)!} \leq$$

$$\leq \frac{(\frac{1}{2}(q-1)n/q-\frac{1}{2})!}{(\frac{1}{2}(q-1)n/q)!} \cdot \frac{(\frac{1}{2}n/q-\frac{1}{2})!}{(\frac{1}{2}n/q)!} \cdot (\tfrac{1}{2}n/q)(q-1)^{\frac{1}{2}} \cdot \frac{(q-1)^{\frac{1}{2}(q-1)n/q}L_t(0)}{(\frac{1}{2}(q-1)n/q-\frac{1}{2})!(\frac{1}{2}n/q-\frac{1}{2})!} \leq$$

$$\leq (\tfrac{1}{2}(q-1)n/q)^{-\frac{1}{2}}(\tfrac{1}{2}n/q)^{\frac{1}{2}}(q-1)^{\frac{1}{2}}(-1)^{\lceil\frac{1}{2}t\rceil}N(0) = (-1)^{\lceil\frac{1}{2}t\rceil}N(0).$$

Due to $L_t(\frac{1}{2}t-1) \leq L_t(\frac{1}{2}t-2)$ and Lemma 2.2.6 one has

$$(-1)^{\lceil \frac{1}{2}t \rceil} N(\tfrac{1}{2}t-1) = \frac{(q-1)^{\frac{1}{2}(q-1)n/q-\frac{1}{4}t+\frac{1}{2}} L_t(\tfrac{1}{2}t-1)}{(\frac{1}{4}(q-1)n/q-\frac{1}{4}t)!\,(\frac{1}{2}n/q+\frac{1}{4}t-1)!} \leq$$

$$\leq \frac{(\frac{1}{2}(q-1)n/q-\frac{1}{4}t+\frac{1}{2})!}{(\frac{1}{2}(q-1)n/q-\frac{1}{4}t+1)!} \cdot \frac{(\frac{1}{2}n/q+\frac{1}{4}t-\frac{3}{2})!}{(\frac{1}{2}n/q+\frac{1}{4}t-1)!} \cdot (\tfrac{1}{2}(q-1)n/q-\tfrac{1}{4}t+1)(q-1)^{-\frac{1}{2}} \cdot$$

$$\cdot \frac{(q-1)^{\frac{1}{2}(q-1)n/q-\frac{1}{4}t+1} L_t(\tfrac{1}{2}t-2)}{(\frac{1}{2}(q-1)n/q-\frac{1}{4}t+\frac{1}{2})!\,(\frac{1}{2}n/q+\frac{1}{4}t-\frac{3}{2})!} \leq$$

$$\leq (\tfrac{1}{2}(q-1)n/q-\tfrac{1}{4}t+1)^{\frac{1}{2}} (\tfrac{1}{2}n/q+\tfrac{1}{4}t-1)^{-\frac{1}{2}} (q-1)^{-\frac{1}{2}} (-1)^{\lceil \frac{1}{2}t \rceil} N(\tfrac{1}{2}t-2) \leq$$

$$\leq (-1)^{\lceil \frac{1}{2}t \rceil} N(\tfrac{1}{2}t-2).$$

since $\frac{1}{4}t-1 \geq 0$.

Thus, it has been proved that $N(x+\frac{1}{2}) - N(x-\frac{1}{2})$ assumes weakly positive as well as weakly negative values for $x \in [-\frac{1}{2}, \frac{1}{2}(t-3)]$. So an $x_0 \in [-\frac{1}{2}, \frac{1}{2}(t-3)]$ exists such that $N(x_0+\frac{1}{2}) = N(x_0-\frac{1}{2})$. □

In the subsequent chapters, we shall speak about "odd", resp. "even" Kravčuk polynomials, whenever alternative 1, resp. 2 holds in the last lemma. Notice that a Kravčuk polynomial of odd degree is odd, but that is has not been proved that a Kravčuk polynomial of even degree is always even.

5.5. Assumptions

We conclude this chapter by a survey of all assumptions made up to now, and the introduction of two new assumptions.

The variables q, n, and t have been assumed to satisfy $q \in \mathbb{N}$, $q \geq 2$, $n \in \mathbb{N}$, $t \in \mathbb{N}$, $t \geq 7$, $t \neq 8$, and $t \leq n$.

Henceforth, it is assumed in addition that $q \geq 3$, *and that a* t*-perfect* q*-ary code of length* n+1 *exists.*

Lemmas 4.3.1 and 3.2.1 yield in this case that K_t has only integral zeros. The restriction $q \geq 3$ is harmless, because of Lemma 4.4.1.

Moreover, it is assumed that $\omega \leq 1/(2t)$, but in Chapter 8 this assumption will be replaced by its counterpart $\omega > 1/(2t)$. Recollect that ω was defined in Section 5.1.

The aim of the next three chapters is to prove that either set of assumptions is inconsistent.

CHAPTER 6

ODD KRAVČUK POLYNOMIALS

In this chapter, very accurate estimates for the distances between the three central zeros of an odd Kravčuk polynomial will be derived. These estimates will be used to prove that the zeros cannot be integral simultaneously.

In this chapter, it is assumed that $\omega \le 1/(2t)$, *and that in Lemma* 5.4.4 *the first alternative holds.*

This implies that odd Kravčuk polynomials with a degree of at least seven, and with relatively large parameter n are considered. For a list of applicable assumptions, the reader is referred to Section 5.5.

6.1. The function C

The first goal is to derive an accurate estimate for the function C introduced at the end of Section 3.3 by

$$C(x) = \frac{v+(q-1)(n-v)-qt}{2(q-1)^{\frac{1}{2}}} \cdot \frac{(\frac{1}{2}v-\frac{1}{2})!(\frac{1}{2}n-\frac{1}{2}v-\frac{1}{2})!}{(\frac{1}{2}v)!(\frac{1}{2}n-\frac{1}{2}v)!},$$

where $x = (q-1)n/q-v$.

LEMMA 6.1.1. *Let* x *be such that* $|x| \le \frac{3.55}{\omega}$. *Then*

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

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

$$+ \frac{(q-2)\omega^4 x}{q(2t+1)^2} - \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + B(.0468\,\frac{\omega^6|x|^3}{(2t+1)^3}) +$$

$$+ B(.0351\,\frac{\omega^4|x|}{(2t+1)^2}) + B(.3698\,\frac{\omega^6}{(2t+1)^3}).$$

PROOF. Firstly, lower bounds for n-v and v are derived. Since

$$\frac{2(q-1)\omega^2|x|}{q(2t+1)} \le 3.55\,\frac{2\omega}{2t+1} \le \frac{3.55}{t(2t+1)} \le .0339,$$

one has

$$n-v = \frac{n}{q}+x = \frac{q(2t+1)}{2(q-1)\omega^2}\left(1+\frac{2(q-1)\omega^2 x}{q(2t+1)}\right) \ge$$

$$\ge \frac{q(2t+1)}{2(q-1)\omega^2}(1-.0339) \ge .4830\,\frac{q(2t+1)}{(q-1)\omega^2},$$

and

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

$$\ge \frac{q(2t+1)}{2\omega^2}(1-.0339) \ge .4830\,\frac{q(2t+1)}{\omega^2}.$$

Hence, by Lemmas 2.2.6 and 2.2.1,

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

$$= -\tfrac{1}{2}\log(\tfrac{1}{2}v) - \tfrac{1}{2}\log(\tfrac{1}{2}(n-v)) - \frac{1}{4v} - \frac{1}{4(n-v)} + \mathcal{B}\left(\frac{1}{24v^3}\right) + \mathcal{B}\left(\frac{1}{24(n-v)^3}\right) =$$

$$= -\tfrac{1}{2}\log\left(\frac{q(2t+1)}{4\omega^2}\left(1-\frac{2\omega^2 x}{q(2t+1)}\right)\right) - \tfrac{1}{2}\log\left(\frac{q(2t+1)}{4(q-1)\omega^2}\left(1+\frac{2(q-1)\omega^2 x}{q(2t+1)}\right)\right) +$$

$$- \frac{\omega^2}{2q(2t+1)}\left(1-\frac{2\omega^2 x}{q(2t+1)}\right)^{-1} - \frac{(q-1)\omega^2}{2q(2t+1)}\left(1+\frac{2(q-1)\omega^2 x}{q(2t+1)}\right)^{-1} +$$

$$+ \mathcal{B}\left(\frac{\omega^6}{24(.4830)^3 q^3 (2t+1)^3}\right) + \mathcal{B}\left(\frac{(q-1)^3\omega^6}{24(.4830)^3 q^3 (2t+1)^3}\right) =$$

$$= -\tfrac{1}{2}\log\frac{q^2(2t+1)^2}{16(q-1)\omega^4} + \frac{\omega^2 x}{q(2t+1)} + \frac{\omega^4 x^2}{q^2(2t+1)^2} +$$

$$+ \frac{4\omega^6 x^3}{3q^3(2t+1)^3}\left(1-\mathcal{B}\left(\frac{2\omega^2|x|}{q(2t+1)}\right)\right)^{-1} - \frac{(q-1)\omega^2 x}{q(2t+1)} + \frac{(q-1)^2\omega^4 x^2}{q^2(2t+1)^2} +$$

$$- \frac{4(q-1)^3\omega^6 x^3}{3q^3(2t+1)^3}\left(1-\mathcal{B}\left(\frac{2(q-1)\omega^2|x|}{q(2t+1)}\right)\right)^{-1} - \frac{\omega^2}{2q(2t+1)} +$$

$$- \frac{\omega^4 x}{q^2(2t+1)^2}\,(1 - \frac{2\omega^2 x}{q(2t+1)})^{-1} - \frac{(q-1)\omega^2}{2q(2t+1)} +$$

$$+ \frac{(q-1)^2\omega^4 x}{q^2(2t+1)^2}\,(1 + \frac{2(q-1)\omega^2 x}{q(2t+1)})^{-1} + B(\frac{\omega^6}{24(.4830)^3(2t+1)^3}).$$

Using

$$(1 - B(\frac{2(q-1)\omega^2|x|}{q(2t+1)}))^{-1} = (1 + B(.0339))^{-1} = 1 + B(.0351),$$

and a fortiori

$$(1 - B(\frac{2\omega^2|x|}{q(2t+1)}))^{-1} = 1 + B(.0351),$$

one finds

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

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

$$- \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + B(\frac{4\cdot.0351\omega^6|x|^3}{3(2t+1)^3}) - \frac{\omega^2}{2(2t+1)} +$$

$$+ \frac{(q-2)\omega^4 x}{q(2t+1)^2} + B(\frac{.0351\omega^4|x|}{(2t+1)^2}) + B(\frac{.3698\omega^6}{(2t+1)^3}) =$$

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

$$+ \frac{(q-2)\omega^4 x}{q(2t+1)^2} - \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + B(.0468\frac{\omega^6|x|^3}{(2t+1)^3}) +$$

$$+ B(.0351\frac{\omega^4|x|}{(2t+1)^2}) + B(.3698\frac{\omega^6}{(2t+1)^3}). \quad \square$$

Next, the other factor occuring in the definition of C(x) is estimated.

LEMMA 6.1.2. *Let* x *be such that* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{3.8715}{\omega t}$. *Then*

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

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

$$+ \frac{(q-2)\omega^4 tx}{q(2t+1)^2} - \frac{\omega^4 t^2}{2(2t+1)^2} + \frac{\omega^6 t^3}{3(2t+1)^3} (\frac{(q-2)x}{qt} - 1)^3(1 + B(.0189)).$$

PROOF. From the expressions for v and n-v derived in the beginning of the proof of Lemma 6.1.1 it follows that

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

$$= \frac{q(2t+1)}{2\omega^2(q-1)^{\frac{1}{2}}} (\frac{1}{2}(1 - \frac{2\omega^2 x}{q(2t+1)}) + \frac{1}{2}(1 + \frac{2(q-1)\omega^2 x}{q(2t+1)}) - \frac{\omega^2 t}{2t+1}) =$$

$$= \frac{q(2t+1)}{2\omega^2(q-1)^{\frac{1}{2}}} (1 + \frac{\omega^2 t}{2t+1} (\frac{(q-2)x}{qt} - 1)).$$

Hence, by Lemma 2.2.1,

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

$$= \log \frac{q(2t+1)}{2\omega^2(q-1)^{\frac{1}{2}}} + \frac{\omega^2 t}{2t+1} (\frac{(q-2)x}{qt} - 1) - \frac{\omega^4 t^2}{2(2t+1)^2} (\frac{(q-2)x}{qt} - 1)^2 +$$

$$+ \frac{\omega^6 t^3}{3(2t+1)^3} (\frac{(q-2)x}{qt} - 1)^3(1 + B(\frac{\omega^2 t}{2t+1}\left|\frac{(q-2)x}{qt} - 1\right|))^{-1} =$$

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

$$+ \frac{(q-2)\omega^4 tx}{q(2t+1)^2} - \frac{\omega^4 t^2}{2(2t+1)^2} + \frac{\omega^6 t^3}{3(2t+1)^3} (\frac{(q-2)x}{qt} - 1)^3(1 + B(.0189)),$$

because of

$$(1 + B(\frac{\omega^2 t}{2t+1}\left|\frac{(q-2)x}{qt} - 1\right|))^{-1} = (1 + B(\frac{3.8715}{2t(2t+1)}))^{-1} =$$

$$= (1 + B(.0185))^{-1} = 1 + B(.0189). \quad \square$$

By combining the Lemmas 6.1.1 and 6.1.2, an estimate for C(x) is found.

LEMMA 6.1.3. *Let* x *be such that* $|x| \le \frac{3.55}{\omega}$ *and* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{3.8715}{\omega t}$. *Then*

$$\log C(x) =$$

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

$$- \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + \frac{\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)x}{qt} - 1\right)^3(1 + B(.0189)) +$$

$$+ B\left(.0468\frac{\omega^6|x|^3}{(2t+1)^3}\right) + B\left(.0351\frac{\omega^4|x|}{(2t+1)^2}\right) + B\left(.3698\frac{\omega^6}{(2t+1)^3}\right).$$

This sharp estimate for C(x) will be used in the next section, but first upper and lower bounds are derived which are independent of x. Define ω_1 and ω_2 by

$$\omega_1 = .9610\omega$$

and

$$\omega_2 = 1.0103\omega$$

LEMMA 6.1.4. *Let* x *be such that* $|\omega| \le \frac{3.55}{\omega}$ *and* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{3.8715}{\omega t}$. *Then*

$$2\cos\omega_2 \le C(x) \le 2\cos\omega_1.$$

PROOF. Define θ by

$$\log C(x) = \log 2 - \theta\omega^2.$$

Then

$$\theta = \tfrac{1}{2} - \frac{1}{(2t+1)^2}\left(\tfrac{1}{2}\omega^2 x^2 + \frac{(q-2)\omega^2(t+1)x}{q} - \tfrac{1}{2}\omega^2 t^2 +\right.$$

$$- \frac{4(q-2)(q^2-q+1)\omega^4 x^3}{3q^3(2t+1)} + \frac{\omega^4 t^3}{3(2t+1)}\left(\frac{(q-2)x}{qt} - 1\right)^3(1 + B(.0189)) +$$

$$\left. + B\left(.0468\,\frac{\omega^4|x|^3}{2t+1}\right) + B(.0351\omega^2|x|) + B\left(.3698\frac{\omega^4}{2t+1}\right)\right).$$

One has the following estimates:

$$\left|\frac{\omega^4 t^3}{3(2t+1)}\left(\frac{(q-2)x}{qt}-1\right)^3(1+B(.0189))\right| \le 1.0189\frac{\omega^4 t^3}{3(2t+1)}\left(\frac{3.8715}{\omega t}\right)^3 \le$$

$$\le 19.71\frac{\omega}{2t+1} \le \frac{19.71}{2t(2t+1)} \le .0939,$$

$$.0468\frac{\omega^4|x|^3}{2t+1} \le .0468\frac{\omega^4}{2t+1}\left(\frac{3.55}{\omega}\right)^3 \le 2.094\frac{\omega}{2t+1} \le \frac{2.094}{2t(2t+1)} \le .0100,$$

$$.0351\omega^2|x| \le .0351\cdot 3.55\omega \le \frac{.1247}{2t} \le .0090,$$

$$.3698\frac{\omega^4}{2t+1} \le \frac{.3698}{16t^4(2t+1)} \le .0001.$$

Hence,

$$\theta = \tfrac{1}{2} - \frac{1}{(2t+1)^2}\left(\tfrac{1}{2}\omega^2x^2 - \tfrac{1}{2}\omega^2t^2 + \frac{(q-2)\omega^2(t+1)x}{q}\left(1 - \frac{4(q^2-q+1)\omega^2x^2}{3q^2(t+1)(2t+1)}\right)+\right.$$

$$\left. + B(.1130)\right).$$

Also

$$0 \le \tfrac{1}{2}\omega^2x^2 \le \tfrac{1}{2}(3.55)^2 \le 6.3013,$$

$$0 \le \tfrac{1}{2}\omega^2t^2 \le \frac{1}{8} = .1250,$$

$$\left|\frac{(q-2)\omega^2(t+1)x}{q}\right| \le 3.55\omega(t+1) \le \frac{3.55(t+1)}{2t} \le 2.0286,$$

$$0 \le \frac{4(q^2-q+1)\omega^2x^2}{3q^2(t+1)(2t+1)} \le \frac{4(3.55)^2}{3(t+1)(2t+1)} \le .1401 \le 2.$$

Hence,

$$\theta \ge \tfrac{1}{2} - \frac{6.3013 + 2.0286 + .1130}{(2t+1)^2} \ge .5 - .0376 = .4624,$$

and

$$\theta \le \tfrac{1}{2} + \frac{.1250 + 2.0286 + .1130}{(2t+1)^2} \le .5 + .0101 = .5101.$$

So

$$\log 2 - .5101\omega^2 \le \log C(x) \le \log 2 - .4624\omega^2,$$

i.e.

$$\exp(-.5101\omega^2) \le \tfrac{1}{2}C(x) \le \exp(-.4624\omega^2).$$

Since

$$\exp(-.5101\omega^2) \ge 1 - .5101\omega^2$$

and

$$\exp(-.4624\omega^2) \le 1 - .4624\omega^2\left(1 - \frac{.4624\omega^2}{2}\right) \le$$

$$\le 1 - .4624\omega^2\left(1 - \frac{.4624}{8t^2}\right) \le 1 - .4618\omega^2,$$

one has

$$1 - .5101\omega^2 \le \tfrac{1}{2}C(x) \le 1 - .4618\omega^2.$$

Since

$$\cos(.9610\omega) \ge 1 - \frac{(.9610)^2\omega^2}{2} \ge 1 - .4618\omega^2$$

and

$$\cos(1.0103\omega) \le 1 - \frac{(1.0103)^2\omega^2}{2}\left(1 - \frac{(1.0103)^2\omega^2}{12}\right) \le$$

$$\le 1 - \frac{(1.0103)^2\omega^2}{2}\left(1 - \frac{(1.0103)^2}{48t^2}\right) \le 1 - .5101\omega^2,$$

one arrives at

$$2\cos(1.0103\omega) \le C(x) \le 2\cos(.9610\omega).$$

The lemma follows by the definitions of ω_1 and ω_2. □

6.2. The functions A and B

As stated previously, N is assumed to have a zero in the interval $[-1, \frac{1}{2}(t-1)]$. Denote this zero by x_0. Define y by

$$y = x - x_0,$$

and the functions A and B by

$$A(y) = C(x)$$

and

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

In the next lemmas, it will be assumed consistently that $|y| \le \frac{3.3}{\omega}$. First, the hypotheses of the Lemmas 6.1.3 and 6.1.4 are verified under this assumption.

$$|x| \le |y| + |x_0| \le \frac{3.3}{\omega} + \tfrac{1}{2}(t-1) \le \frac{3.3}{\omega} + \frac{1}{4\omega} = \frac{3.55}{\omega},$$

$$\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{(q-2)|y|}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right| \le \frac{3.3}{\omega t} + \left|\frac{-1}{t} - 1\right| =$$

$$= \frac{1}{\omega t}(3.3 + \omega(t+1)) \le \frac{1}{\omega t}(3.3 + \frac{t+1}{2t}) \le \frac{3.8715}{\omega t}.$$

Hence, the next lemma follows at once from Lemma 6.1.4.

LEMMA 6.2.1. *Let* $|y| \le \frac{3.3}{\omega}$. *Then*

$$2 \cos \omega_2 \le A(y) \le 2 \cos \omega_1.$$

The next aim is to estimate A(y) - B(y).

LEMMA 6.2.2. *Let* $y \in [\frac{1}{2}, \frac{3.3}{\omega}]$. *Then*

$$\log A(y) - \log B(y) =$$

$$= \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} + \frac{x_0}{t} - \frac{(q-2)\omega^2 y^2}{qt(2t+1)} - \frac{4(q-2)(q^2-q+1)\omega^2 x_0^2}{q^3 t(2t+1)} + \right.$$

$$\left. + \frac{(q-2)\omega^2 t}{q(2t+1)}\left(\frac{(q-2)x_0}{qt} - 1\right)^2 + B(.0358)\right).$$

(In fact, the estimate will be used only for $y \in [1, \frac{3.3}{\omega}]$. The larger interval is taken for reasons of consistency with the next chapter.)

PROOF. By Lemma 6.1.3 it is known that

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

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

$$- \frac{4(q-2)(q^2-q+1)\omega^6(y+x_0)^3}{3q^3(2t+1)^3} +$$

$$+ \frac{\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)y}{qt} + \frac{(q-2)x_0}{qt} - 1\right)^3(1 + B(.0189)) +$$

$$+ B\left(.0468\,\frac{\omega^6|y+x_0|^3}{(2t+1)^3}\right) + B\left(.0351\,\frac{\omega^4|y+x_0|}{(2t+1)^2}\right) + B\left(.3698\,\frac{\omega^6}{(2t+1)^3}\right).$$

This estimate even holds for all y with $|y| \le \frac{3.3}{\omega}$. Hence, for $y \in [\frac{1}{2}, \frac{3.3}{\omega}]$,

$$\log A(y) - \log B(y) = \log A(y) - \log A(-y) =$$

$$= \frac{2(q-2)(t+1)\omega^4 y}{q(2t+1)^2} + \frac{2\omega^4 x_0 y}{(2t+1)^2} - \frac{8(q-2)(q^2-q+1)\omega^6(y^3+3x_0^2y)}{3q^3(2t+1)^3} +$$

$$+ \frac{2\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)^3y^3}{q^3t^3} + \frac{3(q-2)y}{qt}\left(\frac{(q-2)x_0}{qt} - 1\right)^2\right) +$$

$$+ B\left(.0189\,\frac{2\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)y}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right|\right)^3\right) +$$

$$+ B\left(.0468\,\frac{2\omega^6(y+|x_0|)^3}{(2t+1)^3}\right) + B\left(.0351\,\frac{2\omega^4(y+|x_0|)}{(2t+1)^2}\right) +$$

$$+ B\left(.3698\,\frac{2\omega^6}{(2t+1)^3}\right) =$$

$$= \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} + \frac{x_0}{t} - \frac{4(q-2)(q^2-q+1)\omega^2(y^2+3x_0^2)}{3q^3t(2t+1)} +\right.$$

$$\left. + \frac{\omega^2 t^2}{3(2t+1)}\left(\frac{(q-2)^3y^2}{q^3t^3} + \frac{3(q-2)}{qt}\left(\frac{(q-2)x_0}{qt} - 1\right)^2\right) +\right.$$

$$+ B\left(.0063\frac{\omega^2 t^2}{(2t+1)y}\left(\frac{(q-2)y}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right|\right)^3\right) +$$

$$+ B\left(.0468\frac{\omega^2(y+|x_0|)^3}{t(2t+1)y}\right) + B\left(.0351\frac{y+|x_0|}{ty}\right) +$$

$$+ B\left(.3698\frac{\omega^2}{t(2t+1)y}\right)) =$$

$$= \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} + \frac{x_0}{t} - \frac{4(q-2)(q^2-q+1)\omega^2 y^2}{3q^3 t(2t+1)} + \right.$$

$$- \frac{4(q-2)(q^2-q+1)\omega^2 x_0^2}{q^3 t(2t+1)} + \frac{(q-2)^3\omega^2 y^2}{3q^3 t(2t+1)} +$$

$$\left. + \frac{(q-2)\omega^2 t}{q(2t+1)}\left(\frac{(q-2)x_0}{qt} - 1\right)^2 + B(R(y))\right),$$

where R is defined by

$$R(y) = .0063\frac{\omega^2 t^2}{(2t+1)y}\left(\frac{(q-2)y}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right|\right)^3 +$$

$$+ .0468\frac{\omega^2(y+|x_0|)^3}{t(2t+1)y} + .0351\frac{y+|x_0|}{ty} + .3698\frac{\omega^2}{t(2t+1)y}.$$

The function R is obviously convex on $[\frac{1}{2}, \frac{3.3}{\omega}]$, so its maximum is achieved in one of the boundary points of the interval. For $y = \frac{1}{2}$ one has

$$y + |x_0| \le \tfrac{1}{2} + \tfrac{1}{2}(t-1) = \tfrac{1}{2}t,$$

so

$$.0063\frac{\omega^2 t^2}{(2t+1)y}\left(\frac{(q-2)y}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right|\right)^3 \le .0063\frac{1}{2(2t+1)}\left(\frac{1}{2t} + \frac{t+1}{t}\right)^3 =$$

$$= .0063\frac{(2t+3)^3}{16t^3(2t+1)} \le .0004,$$

$$.0468\frac{\omega^2(y+|x_0|)^3}{t(2t+1)y} \le .0468\frac{1}{16(2t+1)} \le .0002,$$

$$.0351\frac{y+|x_0|}{ty} \le .0351,$$

$$.3698\frac{\omega^2}{t(2t+1)y} \le \frac{.3698}{2t^3(2t+1)} \le .0001.$$

Hence,

$$R(\tfrac{1}{2}) \le .0358.$$

For $y = \frac{3.3}{\omega}$, one has $y + |x_0| \le \frac{3.55}{\omega}$, so

$$.0063\frac{\omega^2 t^2}{(2t+1)y}\left(\frac{(q-2)y}{qy} + \left|\frac{(q-2)x_0}{qt} - 1\right|\right)^3 \le$$

$$\le .0063\frac{\omega^3 t^2}{3.3(2t+1)}\left(\frac{3.8715}{\omega t}\right)^3 \le \frac{.1108}{t(2t+1)} \le .0011,$$

$$.0468\frac{\omega^2(y+|x_0|)^3}{t(2t+1)y} \le .0468\frac{\omega^3}{3.3t(2t+1)}\left(\frac{3.55}{\omega}\right)^3 \le \frac{.6345}{t(2t+1)} \le .0061,$$

$$.0351\frac{y+|x_0|}{ty} \le .0351\frac{3.55}{3.3t} \le .0054,$$

$$.3698\frac{\omega^2}{t(2t+1)y} \le .0001.$$

Hence

$$R(\tfrac{3.3}{\omega}) \le .0127.$$

Thus, it is known $R(y) \le .0358$ for $y \in [\frac{1}{2}, \frac{3.3}{\omega}]$, and therefore,

$$\log A(y) - \log B(y) =$$

$$= \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} + \frac{x_0}{t} - \frac{(q-2)\omega^2 y^2}{qt(2t+1)} - \frac{4(q-2)(q^2-q+1)\omega^2 x_0^2}{q^3 t(2t+1)} + \right.$$

$$\left. + \frac{(q-2)\omega^2 t}{q(2t+1)}\left(\frac{(q-2)x_0}{qt} - 1\right)^2 + B(.0358)\right). \quad \square$$

From Lemma 6.2.2, lower and upper bounds for A(y) - B(y) are deduced.

LEMMA 6.2.3. *Let* $y \in [\frac{1}{2}, \frac{3.3}{\omega}]$. *Then*

$$A(y) > B(y).$$

PROOF. From Lemma 6.2.2, it follows that

$$\log A(y) - \log B(y) \geq$$

$$\geq \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} - \frac{1}{t} - \frac{(3.3)^2(q-2)}{qt(2t+1)} - \frac{(q-2)(q^2-q+1)(t-1)^2}{4q^3t^3(2t+1)} + \right.$$

$$\left. - .0358\right) \geq$$

$$\geq \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{q-2}{q}\left(\frac{t+1}{t} - \frac{10.89}{t(2t+1)} - \frac{(t-1)^2}{4t^3(2t+1)}\right) - \frac{1}{t} - .0358\right) \geq$$

$$\geq \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{1}{3}(1 - .1038 - .0018) - .1787\right) \geq .1194\,\frac{2\omega^4 ty}{(2t+1)^2} > 0. \quad \square$$

LEMMA 6.2.4. *Let* $y \in [\frac{1}{2}, \frac{3.3}{\omega}]$. *Then*

$$A(y) - B(y) \leq .2008\omega^4 y.$$

PROOF. From Lemma 6.2.2, it follows that

$$\log A(y) - \log B(y) \leq \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{t+1}{t} + \frac{t-1}{2t} + \frac{\omega^2 t}{2t+1}\left(\frac{t+1}{t}\right)^2 + .0358\right) \leq$$

$$\leq \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{3t+1}{2t} + \frac{(t+1)^2}{4t^3(2t+1)} + .0358\right) \leq$$

$$\leq .0623\omega^4 y(1.5715 + .0032 + .0358) \leq .1004\omega^4 y.$$

Consequently, since $A(y) = C(x) \leq 2$ by Lemma 6.1.4,

$$A(y) - B(y) = A(y)(1 - \frac{B(y)}{A(y)}) \leq 2(1 - \exp(-.1004\omega^4 y)) \leq$$

$$\leq .2008\omega^4 y. \quad \square$$

6.3. The three central zeros

From Lemma 3.3.4, it is known that N is a function which satisfies the three term recurrence relation

$$N(x+1) - C(x)N(x) + N(x-1) = 0$$

Furthermore, N is assumed to have a zero in x_0. It follows from Lemma 3.3.2 that $N(x_0+1) \neq 0$. Hence the function F can be defined by

$$F(y) = \frac{N(x)}{N(x_0+1)} .$$

Then $F(0) = 0$, $F(1) = 1$, and F satisfies the recurrence relation

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

F has integral zeros, due to the integrality of the zeros of K_t. Next, define y_1 as being the smallest zero of F in the interval $(0,\pi/\omega_1\rfloor$, provided such a zero exists; otherwise, define $y_1 = \lfloor \pi/\omega_1 \rfloor + 1$. Observe that in any case $F(y_1) \geq 0$.

LEMMA 6.3.1.

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

$$F(y) \leq \frac{\sin(\omega_1 y)}{\sin \omega_1} \quad \textit{for } y \in [0,1,y_1],$$

$$F(y) \geq \frac{\sin(\omega_2 y)}{\sin \omega_2} \quad \textit{for } y \in [0,1,\frac{\pi}{\omega_2}],$$

$$\frac{\pi}{\omega_2} \leq y_1 \leq \frac{\pi}{\omega_1},$$

and

$$y_1 \textit{ is the smallest positive zero of } F.$$

PROOF. $y_1 \in \mathbb{Z}$ is obvious from the integrality of the zeros of F, resp. of $\lfloor \pi/\omega_1 \rfloor + 1$. Next, observe that

$$y_1 - 1 \leq \frac{\pi}{\omega_1} = \frac{\pi}{.9610\omega} \leq \frac{3.3}{\omega},$$

so Lemma 6.2.1 yields that $2 \cos \omega_2 \leq A(y) \leq 2 \cos \omega_1$ for $y \in [0,1,y_1)$.

Define the function G by

$$G(y) = \frac{\sin(\omega_1 y)}{\sin \omega_1}.$$

Then $G(0) = 0$, $G(1) = 1$, and G satisfies the recurrence relation

$$G(y+1) - 2 \cos \omega_1 \, G(y) + G(y-1) = 0.$$

Now the second assertion of the lemma follows from Lemma 2.4.3 with $a = 1$, $b = y_1$, and $B(y) = 2 \cos \omega_1$. Since $G(\lfloor \pi/\omega_1 \rfloor + 1) < 0$, the "otherwise"-part in the definition of y_1 does not apply, which proves $y_1 \leq \pi/\omega_1$ and the fifth assertion of the lemma.

Defining G by

$$G(y) = \frac{\sin(\omega_2 y)}{\sin \omega_2},$$

the third assertion follows in a similar way from Lemma 2.4.3 with $a = 1$, $b = \lfloor \pi/\omega_2 \rfloor$, and with F and G interchanged. This proves in turn that $y_1 \geq \pi/\omega_2$. □

The lower bound for F which was established in Lemma 6.3.1 can be improved in a neighbourhood of y_1.

Define

$$\eta = \left\lceil \frac{\pi}{2\omega_1} \right\rceil.$$

LEMMA 6.3.2.

$$\eta \le \frac{1.7060}{\omega},$$

$$F(y) \ge .5734y \qquad \textit{for } y \in [0,1,\eta],$$

and

$$F(y) \ge \frac{.9782}{\omega} \sin(\omega_1(y_1-y)) \textit{ for } y \in [\eta,1,y_1].$$

PROOF. First, bounds for η are derived.

$$\frac{\pi}{2\omega_1} \le \eta \le \frac{\pi}{2\omega_1} + 1 \le \frac{\pi}{1.9220\omega} + \frac{1}{2\omega t} \le \frac{1.7060}{\omega}.$$

So

$$\frac{\pi}{2} \le \omega_1\eta \le \omega_2\eta \le 1.0103 \cdot 1.7060 \le 1.7236 \le \pi.$$

Hence, by Lemma 6.3.1,

$$F(\eta) \ge \frac{\sin(\omega_2\eta)}{\sin\ \omega_2} \ge \frac{\sin\ 1.7236}{1.0103\omega} \ge \frac{.9782}{\omega},$$

and for $y \in [0,1,\eta]$,

$$F(y) \ge \frac{\sin(\omega_2 y)}{\sin\ \omega_2} \ge \frac{y\ \sin(\omega_2\eta)}{\omega_2\eta} \ge \frac{y\ \sin\ 1.7236}{1.7236} \ge .5734y,$$

proving the second assertion of the lemma.

Next, define the function G by

$$G(y) = \frac{.9782}{\omega} \sin(\omega_1(y_1-y)).$$

Then

$$F(\eta) \ge \frac{.9782}{\omega} \ge G(\eta),$$

and

$$F(y_1) = 0 = G(y_1).$$

Now the third assertion of the lemma follows from Lemma 2.4.4 with $a = \eta$, $b = y_1$, and from Lemma 6.2.1. □

In the remainder of this section, the function G is defined by

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

Then $G(0) = 0$, $G(1) = 1$, and G satisfies the recurrence relation

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

Furthermore, G has integral zeros. Next, define z_1 as being the smallest zero of G in the interval $(0,y_1)$, provided such a zero exists; otherwise, define $z_1 = y_1$. In any case, $G(z_1) \geq 0$.

LEMMA 6.3.3.

$$z_1 \in \mathbb{Z},$$

$$G(y) < F(y) \qquad \textit{for } y \in (1,1,z_1],$$

$$z_1 < y_1,$$

and

z_1 *is the smallest positive zero of* G.

PROOF. $z_1 \in \mathbb{Z}$ is obvious from the integrality of the zeros of G. Since $z_1 \leq y_1 \leq 3.3/\omega$, Lemma 6.2.3 applies. The second assertion of the lemma follows from Lemma 2.4.3 with $a = 1$, $b = z_1$, and F and G interchanged. Since $F(y_1) = 0$, the "otherwise"-part in the definition of z_1 does not apply, which proves the third and fourth assertion of the lemma. □

A lower bound for z_1 is established by applying Lemma 2.4.1.

LEMMA 6.3.4.

$$z_1 > y_1 - 1.$$

PROOF. First, the functions α, β, and γ as defined in Lemma 2.4.1 are estimated. Lemmas 6.2.4, 6.3.1, and 6.3.3 yield for $k \in [1,1,y_1-1]$:

$$\alpha(k) = (A(k) - B(k))F(k)G(k) \le .2008\omega^4 k \frac{\sin^2(\omega_1 k)}{\sin^2\omega_1}.$$

Since

$$\frac{\sin \omega_1}{\omega_1} \ge 1 - \frac{1}{6}\omega_1^2 \ge 1 - \frac{(.9610)^2}{24t^2} \ge .9992,$$

it follows that

$$\alpha(k) \le .2008\omega^4 k \frac{\sin^2(\omega_1 k)}{(.9992)^2\omega_1^2} \le \frac{.2012\omega^2 k}{(.9610)^2} \sin^2(\omega_1 k) \le$$

$$\le .2179\omega^2 k \sin^2(\omega_1 k).$$

For $k \in [1,1,y_1-1]$, one has by Lemma 2.2.4:

$$\beta(k) = \sum_{i\in[1,1,k)} \alpha(i) \le .2179\omega^2 \sum_{i=1}^{k-1} i \sin^2(\omega_1 i) \le .2179\omega^2 \frac{1}{4}\left\lceil\frac{\pi}{\omega_1}\right\rceil^2 \le$$

$$\le .0545\omega^2\left(\frac{3.2691}{\omega} + 1\right)^2 \le .0545(3.2691 + \frac{1}{2t})^2 \le .6082.$$

For $k \in [1,1,\eta]$, the following estimate is better (cf. Lemma 2.2.2):

$$\beta(k) \le .2179\omega^2\omega_1^2 \sum_{i=1}^{k-1} i^3 = .2179(.9610)^2\omega^4 \frac{1}{4}k^2(k-1)^2 \le$$

$$\le .0504\omega^4 k^2(k-1)^2.$$

Hence, by Lemma 6.3.2 one has for $k \in [1,1,\eta]$:

$$\gamma(k) = \sum_{i\in(1,1,k]} \frac{\beta(i)}{F(i)F(i-1)} \le \frac{.0504\omega^4}{(.5734)^2} \sum_{i=2}^{\eta} \frac{i^2(i-1)^2}{i(i-1)} \le$$

$$\le .1533\omega^4 \sum_{i=2}^{\eta} i(i-1) = .1533\omega^4 \frac{1}{3}\eta(\eta+1)(\eta-1) \le .0511\omega^4\eta^3 \le$$

$$\le \frac{.0511(1.7060)^3}{2t} \le .0182.$$

For $k \in [\eta,1,y_1-1]$, one deduces from Lemmas 6.3.2 and 2.2.5:

$$\gamma(k) - \gamma(\eta) = \sum_{i\in(\eta,1,k]} \frac{\beta(i)}{F(i)F(i-1)} \leq$$

$$\leq \frac{.6082}{(.9782)^2}\omega^2 \sum_{i=\eta+1}^{y_1-1} \frac{1}{\sin(\omega_1(y_1-i))\sin(\omega_1(y_1-i+1))} \leq$$

$$\leq .6357\omega^2 \sum_{j=2}^{y_1-\eta} \frac{1}{\sin(\omega_1 j)\sin(\omega_1(j-1))} \leq .6357\frac{\omega^2}{\omega_1^2} = \frac{.6357}{(.9610)^2} \leq$$

$$\leq .6884.$$

Hence, for $k \in [1,1,y_1-1]$:

$$\gamma(k) \leq .0182 + .6884 = .7066.$$

Now Lemma 2.4.1 gives that

$$G(k) \geq .2934F(k) > 0,$$

for $k \in [1,1,y_1-1]$. Hence $z_1 > y_1-1$, proving the lemma. □

The assertions $y_1 \in \mathbb{Z}$ (Lemma 6.3.1), $z_1 \in \mathbb{Z}$ (Lemma 6.3.3), $z_1 < y_1$ (Lemma 6.3.3), and $z_1 > y_1-1$ (Lemma 6.3.4) are clearly contradictory. This proves

LEMMA 6.3.5. *The assumptions made in this chapter are inconsistent.*

CHAPTER 7

EVEN KRAVČUK POLYNOMIALS

The crucial difference between odd and even Kravčuk polynomials is that the former have a zero very close to $(q-1)n/q$, whereas the latter have two consecutive zeros which are almost symmetric around $(q-1)n/q$. In this chapter, very accurate estimates for the distances between these two zeros and their "outer" neighbours will be established. These estimates will be used to prove that the four zeros cannot be integral simultaneously.

In this entire chapter, it is assumed that $\omega \le 1/(2t)$, *and that in Lemma 5.4.4 the second alternative holds.*

This implies that even Kravčuk polynomials with a degree of at least ten, and with relatively large parameter n are considered. For a list of applicable assumptions, the reader is referred to Section 5.5.

Many derivations in this chapter can almost be copied from the previous chapter, apart from some numerical constants in the estimates. In these cases, the results will be given without further explanation, while in the proofs only the differences with the corresponding proof in the previous chapter will be indicated.

7.1. The function C

LEMMA 7.1.1. *Let* x *be such that* $|x| \le \frac{5.25}{\omega}$. *Then*

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

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

$$+ \frac{(q-2)\omega^4 x}{q(2t+1)^2} - \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + B(.0343\frac{\omega^6|x|^3}{(2t+1)^3}) +$$

$$+ B(.0257\frac{\omega^4|x|}{(2t+1)^2}) + B(.3597\frac{\omega^6}{(2t+1)^3}).$$

PROOF. This is identical to the proof of Lemma 6.1.1 apart from the following changes:

3.55	becomes	5.25
.0339	"	.0250
.4830	"	.4875
.0351	"	.0257
.3698	"	.3597
.0468	"	.0343. □

LEMMA 7.1.2. *Let* x *be such that* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{5.55}{\omega t}$. *Then*

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

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

$$+ \frac{(q-2)\omega^4 tx}{q(2t+1)^2} - \frac{\omega^4 t^2}{2(2t+1)^2} + \frac{\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)x}{qt} - 1\right)^3 (1 + B(.0135)).$$

PROOF. Apply the following changes to the proof of Lemma 6.1.2:

.0189	becomes	.0135
3.8715	"	5.55
.0185	"	.0133. □

LEMMA 7.1.3. *Let* x *be such that* $|x| \le \frac{5.25}{\omega}$ *and* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{5.55}{\omega t}$. *Then*

$$\log C(x) =$$

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

$$- \frac{4(q-2)(q^2-q+1)\omega^6 x^3}{3q^3(2t+1)^3} + \frac{\omega^6 t^3}{3(2t+1)^3}\left(\frac{(q-2)x}{qt} - 1\right)^3 (1 + B(.0135)) +$$

$$+ B\left(.0343\frac{\omega^6|x|^3}{(2t+1)^3}\right) + B\left(.0257\frac{\omega^4|x|}{(2t+1)^2}\right) + B\left(.3597\frac{\omega^6}{(2t+1)^3}\right).$$

Define ω_1 and ω_2 by

$$\omega_1 = .9607\omega$$

and

$$\omega_2 = 1.0073\omega.$$

LEMMA 7.1.4. *Let* x *be such that* $|x| \le \frac{5.25}{\omega}$ *and* $\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{5.55}{\omega t}$. *Then*

$$2 \cos \omega_2 \le C(x) \le 2 \cos \omega_1.$$

PROOF. Apply the following changes to the proof of Lemma 6.1.4:

.0189	becomes	.0135
.0468	"	.0343
.0351	"	.0257
.3698	"	.3597
1.0189	"	1.0135
3.8715	"	5.55
19.71	"	57.76
.0939	"	.1376
3.55	"	5.25
2.094	"	4.964
.0100	"	.0119
.1247	"	.1350
.0090	"	.0068
.1130	"	.1564
6.3013	"	13.7813
2.0286	"	2.8875
.1401	"	.1591
.0376	"	.0382
.4624	"	.4618
.0101	"	.0072
.5101	"	.5072
.4618	"	.4615

.9610 becomes .9607
1.0103 " 1.0073. □

7.2. The functions A and B

Let x_0 be some number in the interval $[-1,\frac{1}{2}(t-1)]$. (In this section this number has no connection with the x_0 in Lemma 5.4.4!) Define y by

$$y = x - x_0$$

and the functions A and B by

$$A(y) = C(x)$$

and

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

In the next lemmas, it will be assumed consistently that $|y| \le \frac{5}{\omega}$. First, the hypotheses of the Lemmas 7.1.3 and 7.1.4 are verified under this assumption.

$$|x| \le |y| + |x_0| \le \frac{5}{\omega} + \frac{t-1}{2} \le \frac{5}{\omega} + \frac{1}{4\omega} = \frac{5.25}{\omega},$$

$$\left|\frac{(q-2)x}{qt} - 1\right| \le \frac{(q-2)|y|}{qt} + \left|\frac{(q-2)x_0}{qt} - 1\right| \le \frac{5}{\omega t} + \left|\frac{-1}{t} - 1\right| =$$

$$= \frac{1}{\omega t}(5 + \omega(t+1)) \le \frac{1}{\omega t}\,(5 + \frac{t+1}{2t}) \le \frac{5.55}{\omega t}.$$

Hence, the next lemma follows at once from Lemma 7.1.4.

LEMMA 7.2.1. *Let* $|y| \le \frac{5}{\omega}$. *Then*

$$2 \cos \omega_2 \le A(y) \le 2 \cos \omega_1.$$

The next aim is to estimate A(y) - B(y).

LEMMA 7.2.2. *Let* $y \in [\frac{1}{2},\frac{5}{\omega}]$. *Then*

$$\log A(y) - \log B(y) =$$

$$= \frac{2\omega^4 ty}{(2t+1)^2}\left(\frac{(q-2)(t+1)}{qt} + \frac{x_0}{t} - \frac{(q-2)\omega^2 y^2}{qt(2t+1)} - \frac{4(q-2)(q^2-q+1)\omega^2 x_0^2}{q^3 t(2t+1)} + \right.$$

$$\left. + \frac{(q-2)\omega^2 t}{q(2t+1)}\left(\frac{(q-2)x_0}{qt} - 1\right)^2 + B(.0262)\right).$$

PROOF. Apply the following changes to the proof of Lemma 6.2.2:

.0189	becomes	.0135
.0468	"	.0343
.0351	"	.0257
.3698	"	.3597
.0063	"	.0045
3.3	"	5
.0004	"	.0002
.0358	"	.0262
3.55	"	5.25
3.8715	"	5.55
.1108	"	.1539
.0011	"	.0008
.6345	"	.9927
.0061	"	.0048
.0054	"	.0027
.0127	"	.0084. □

LEMMA 7.2.3. *Let* $y \in [\frac{1}{2}, \frac{5}{\omega}]$. *Then*

$$A(y) > B(y).$$

PROOF. Apply the following changes to the proof of Lemma 6.2.3:

6.2.2	becomes	7.2.2
.0358	"	.0262
10.89	"	25
.1038	"	.1191
.0018	"	.0010
.1787	"	.1262
.1194	"	.1672. □

LEMMA 7.2.4. *Let* $y \in [\frac{1}{2}, \frac{5}{\omega}]$. *Then*

$$A(y) - B(y) \leq .1434\omega^4 y.$$

PROOF. Apply the following changes to the proof of Lemma 6.2.4:

6.2.2	becomes	7.2.2
.0358	"	.0262
.0623	"	.0454
1.5715	"	1.55
.0032	"	.0015
.1004	"	.0717
6.1.4	"	7.1.4
.2008	"	.1434. □

7.3. The two central zeros

From Lemma 3.3.4, it is known that N is a function which satisfies the three term recurrence relation

$$N(x+1) - C(x)N(x) + N(x-1) = 0.$$

By Lemma 5.4.4, x_0 can be chosen so that $x_0 \in [-\frac{1}{2}, \frac{1}{2}(t-3)]$ and $N(x_0-\frac{1}{2}) = N(x_0+\frac{1}{2})$. With this choice of x_0, the results of Section 7.2 can be applied, since $x_0 \in [-1, \frac{1}{2}(t-1)]$. The definitions of y, A, and B are adopted from that section. Since $N(x_0+\frac{1}{2}) \neq 0$ (cf. Lemma 3.3.2), the function F can be defined by

$$F(y) = \frac{N(x)}{N(x_0+\frac{1}{2})} .$$

Then $F(-\frac{1}{2}) = F(\frac{1}{2}) = 1$, and F satisfies the recurrence relation

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

Next, define y_0 as being the smallest zero of F in the interval $(0, \pi/(2\omega_1)+1)$, provided such a zero exists; otherwise, define $y_0 = \pi/(2\omega_1) + 1$. Notice that anyhow $F(y_0) \geq 0$.

LEMMA 7.3.1.

$$F(y) \le \frac{\cos(\omega_1 y)}{\cos(\frac{1}{2}\omega_1)} \qquad \textit{for} \quad y \in [\tfrac{1}{2},1,y_0],$$

$$y_0 < \frac{\pi}{2\omega_1} + 1 \le \frac{1.6851}{\omega},$$

and

y_0 *is the smallest positive zero of* F.

PROOF. First, observe that

$$y_0 \le \frac{\pi}{2\omega_1} + 1 \le \frac{\pi}{1.9214\omega} + \frac{1}{2\omega t} \le \frac{1.6851}{\omega} \le \frac{5}{\omega},$$

so Lemma 7.2.1 establishes that $2 \cos \omega_2 \le A(y) \le 2 \cos \omega_1$ for $y \in [0,1,y_0]$.

Define the function G by

$$G(y) = \frac{\cos(\omega_1 y)}{\cos(\frac{1}{2}\omega_1)}.$$

Then $G(-\frac{1}{2}) = G(\frac{1}{2}) = 1$, and G satisfies the recurrence relation

$$G(y+1) - 2 \cos \omega_1 \, G(y) + G(y-1) = 0.$$

Now the first assertion of the lemma follows from Lemma 2.4.3 with $a = \frac{1}{2}$, $b = \lfloor y_0 - \frac{1}{2} \rfloor + \frac{1}{2}$, and $B(y) = 2 \cos \omega_1$. Since $G(\lfloor \pi/(2\omega_1) + \frac{1}{2} \rfloor + \frac{1}{2}) < 0$, the "otherwise"-part in the definition of y_0 does not apply, which proves $y_0 < \pi/(2\omega_1) + 1$ and the third assertion of the lemma. □

This time, a rather trivial lower bound for F suffices. Define

$$\eta = \lfloor y_0 - \tfrac{1}{2} \rfloor + \tfrac{1}{2}.$$

LEMMA 7.3.2.

$$\eta \le \frac{1.6851}{\omega},$$

and

$$F(y) \geq \frac{\eta - y}{\eta} \quad \textit{for} \quad y \in [\tfrac{1}{2}, 1, \eta].$$

PROOF. By Lemma 7.3.1, F is weakly positive on $[\frac{1}{2},1,\eta]$. If $y \in [\frac{1}{2},1,\eta]$, then $|y| \leq 5/\omega$, so it follows from Lemma 7.2.1 that $A(y) \leq 2$. Hence, by the recurrence relation derived above, F is concave on $[\frac{1}{2},1,\eta]$. Finally, $F(\frac{1}{2}) = 1$ and $F(\eta) \geq 0$. □

In the remainder of this section, the function G is defined by

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

Then $G(-\frac{1}{2}) = G(\frac{1}{2}) = 1$, and G satisfies the recurrence relation

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

Next, define t_0 as being the smallest zero of G in the interval $(0,y_0+1)$, provided such a zero exists; otherwise, define $z_0 = y_0+1$. Anyhow, $G(z_0) \geq 0$.

LEMMA 7.3.3.

$$G(y) \leq F(y) \quad \textit{for} \quad y \in [\tfrac{1}{2}, 1, z_0],$$

$$z_0 < y_0 + 1,$$

and

z_0 *is the smallest positive zero of* G.

PROOF. First, observe that

$$z_0 \leq y_0 + 1 \leq \frac{\pi}{2\omega_1} + 2 \leq \frac{\pi}{1.9214\omega} + \frac{1}{\omega t} \leq \frac{1.7351}{\omega} \leq \frac{5}{\omega},$$

so Lemma 7.2.3 can be applied. The first assertion of the lemma follows from Lemma 2.4.3 with $a = \frac{1}{2}$, $b = \lfloor z_0 - \frac{1}{2} \rfloor + \frac{1}{2}$, and F and G interchanged. Since $F(\lfloor y_0 + \frac{1}{2} \rfloor + \frac{1}{2}) < 0$, the "otherwise"-part in the definition of z_0 does not apply, which proves the second and third assertion of the lemma. □

A lower bound for z_0, is found by applying Lemma 2.4.1.

LEMMA 7.3.4.

$$z_0 > y_0 - 2.$$

PROOF. First, the functions α, β, and γ as defined in Lemma 2.4.1 are estimated. Lemmas 7.2.4, 7.3.1, and 7.3.3 yield for $k \in [\frac{1}{2},1,\eta-1]$:

$$\alpha(k) = (A(k) - B(k))F(k)G(k) \le .1434\omega^4 k \frac{\cos^2(\omega_1 k)}{\cos^2(\frac{1}{2}\omega_1)} \le .1434\omega^4 k,$$

$$\beta(k) = \sum_{i\in[\frac{1}{2},1,k)} \alpha(i) \le .1434\omega^4 \sum_{i\in[\frac{1}{2},1,\eta)} i \le .0717\omega^4\eta^2,$$

$$\gamma(k) = \sum_{i\in(\frac{1}{2},1,k]} \frac{\beta(i)}{F(i)F(i-1)} \le .0717\omega^4\eta^2 \sum_{i\in(\frac{1}{2},1,\eta-1]} \frac{\eta^2}{(\eta-i)(\eta-i+1)} \le$$

$$\le .0717\omega^4 y_0^4 \le .0717(1.6851)^4 \le .5782.$$

Now Lemma 2.4.1 yields that

$$G(k) \ge .4218F(k) > 0$$

for $k \in [\frac{1}{2},1,\eta-1]$. Hence $z_0 > \eta-1 > y_0-2$. □

Recapitulating, it is now known that N has zeros in x_0+y_0 and x_0-z_0 with $-\frac{1}{2} \le x_0 \le \frac{1}{2}(t-3)$, $0 < y_0 \le \pi/(2\omega_1) + 1$, $z_0 > 0$, and $-1 < y_0-z_0 < 2$.

Define x_0' and y_0' by

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

and

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

Then $-1 < x_0' < \frac{1}{2}(t-1)$, $0 < y_0' < \pi/(2\omega_1) + \frac{3}{2}$, and N has zeros in $x_0' + y_0'$ and $x_0' - y_0'$.

7.4. The adjacent zeros

In this section, x_0 and y_0 are chosen according to $x_0 = x_0'$ and $y_0 = y_0'$, where x_0' and y_0' have been defined at the end of the previous section. Now N has zeros in x_0+y_0 and x_0-y_0. Moreover, the following inequalities concerning x_0 and y_0 are known.

LEMMA 7.4.1.

$$-1 \le x_0 \le \tfrac{1}{2}(t-1),$$

and

$$0 < y_0 < \frac{1.7101}{\omega} .$$

PROOF. Only the last inequality needs explanation. It follows from

$$y_0 < \frac{\pi}{2\omega_1} + \frac{3}{2} \le \frac{\pi}{1.9214\omega} + \frac{3}{4\omega t} \le \frac{1.7101}{\omega} . \quad \square$$

With this new choice of x_0, the results of Section 7.2 are applied again, and the definitions of y, A, and B are adopted again from that section. Since $N(x_0+y_0+1) \neq 0$ (cf. Lemma 3.3.2), the function F can be defined by

$$F(y) = \frac{N(x)}{N(x_0+y_0+1)} .$$

Then $F(y_0) = 0$, $F(y_0+1) = 1$, and F satisfies the recurrence relation

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

Furthermore, the zeros of F have integral differences with y_0, due to the integrality of the zeros of K_t. Next, define y_1 to be the smallest zero of F in the interval $(y_0, y_0+\pi/\omega_1]$, provided such a zero exists; otherwise, define $y_1 = y_0 + \lfloor \pi/\omega_1 \rfloor + 1$. Observe that anyhow $F(y_1) \ge 0$.

LEMMA 7.4.2.

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

$$F(y) \le \frac{\sin(\omega_1(y-y_0))}{\sin \omega_1} \qquad \textit{for } y \in [y_0,1,y_1],$$

$$F(y) \ge \frac{\sin(\omega_2(y-y_0))}{\sin \omega_2} \qquad \textit{for } y \in [y_0,1,y_0+\pi/\omega_1],$$

$$y_1-y_0 \le \frac{\pi}{\omega_1} \le \frac{3.2702}{\omega},$$

and

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

PROOF. $y_1-y_0 \in \mathbb{Z}$ is obvious from the integrality of the zeros of F, resp. of $\lfloor \pi/\omega_1 \rfloor + 1$. Next, observe that

$$y_1-y_0-1 \le \frac{\pi}{\omega_1} \le \frac{\pi}{.9607\omega} \le \frac{3.2702}{\omega}.$$

Hence, by Lemma 7.4.1:

$$y_1-1 \le \frac{1.7101}{\omega} + \frac{3.2702}{\omega} = \frac{4.9803}{\omega} \le \frac{5}{\omega},$$

so Lemma 7.2.1 yields that $2 \cos \omega_2 \le A(y) \le 2 \cos \omega_1$ for $y \in [y_0,1,y_1)$.

Defining the function G respectively by

$$G(y) = \frac{\sin(\omega_1(y-y_0))}{\sin \omega_1},$$

and

$$G(y) = \frac{\sin(\omega_2(y-y_0))}{\sin \omega_2},$$

the second and third assertion of the lemma follow in the same way as in the proof of Lemma 6.3.1. Again, the "otherwise"-part in the definition of y_1 does not apply, which proves the fourth and fifth assertion of the lemma. □

Define η by

$$\eta = y_0 + \lceil \frac{\pi}{2\omega_1} \rceil.$$

LEMMA 7.4.3.

$$\eta - y_0 \le \frac{1.6851}{\omega},$$

$$F(y) \ge .5844(y-y_0) \qquad \textit{for } y \in [y_0, 1, \eta],$$

and

$$F(y) \ge \frac{.9847}{\omega} \sin(\omega_1(y_1 - y)) \qquad \textit{for } y \in [\eta, 1, y_1].$$

PROOF. First, bounds for $\eta - y_0$ are derived.

$$\frac{\pi}{2\omega_1} \le \eta - y_0 \le \frac{\pi}{2\omega_1} + 1 \le \frac{\pi}{1.9214\omega} + \frac{1}{2\omega t} \le \frac{1.6851}{\omega}.$$

So

$$\frac{\pi}{2} \le \omega_1(\eta - y_0) \le \omega_2(\eta - y_0) \le 1.0073 \cdot 1.6851 \le 1.6975 \le \pi.$$

Hence, by Lemma 7.4.2,

$$F(\eta) \ge \frac{\sin(\omega_2(\eta - y_0))}{\sin \omega_2} \ge \frac{\sin 1.6975}{1.0073\omega} \ge \frac{.9847}{\omega},$$

and for $y \in [y_0, 1, \eta]$,

$$F(y) \ge \frac{\sin(\omega_2(y-y_0))}{\sin \omega_2} \ge \frac{(y-y_0)\sin(\omega_2(\eta - y_0))}{\omega_2(\eta - y_0)} \ge$$

$$\ge \frac{(y-y_0)\sin 1.6975}{1.6975} \ge .5843(y-y_0),$$

proving the second assertion of the lemma.

Defining the function G by

$$G(y) = \frac{.9847}{\omega} \sin(\omega_1(y_1 - y)),$$

the third assertion of the lemma follows in the same way as in the proof of Lemma 6.3.2. □

In the remainder of this section, the function G is defined by

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

Then $G(y_0) = 0$, $G(y_0+1) = 1$, and G satisfies the recurrence relation

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

Furthermore, the zeros of G have integral differences with y_0. Next, define z_1 as being the smallest zero of G in the interval (y_0,y_1), provided such a zero exists; otherwise, define $z_1 = y_1$. In any case, $G(z_1) \geq 0$.

LEMMA 7.4.4.

$$z_1-y_0 \in \mathbb{Z},$$

$$G(y) < F(y) \qquad \textit{for } y \in (y_0+1,1,z_1],$$

$$z_1 < y_1,$$

and

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

PROOF. $z_1-y_0 \in \mathbb{Z}$ follows from the integrality of the zeros of K_t. Since $z_1 \leq y_1 = y_0 + (y_1-y_0) \leq \frac{1.7101}{\omega} + \frac{3.2702}{\omega} = \frac{4.9803}{\omega} \leq \frac{5}{\omega}$ (cf. Lemma 7.4.1 and 7.4.2), Lemma 7.2.3 can be applied. The second assertion of the lemma follows from Lemma 2.4.3 with $a = y_0+1$ and $b = z_1$, and F and G interchanged. Since $F(y_1) = 0$, the "otherwise"-part in the definition of z_1 does not apply, which proves the third and fourth assertion of the lemma. □

LEMMA 7.4.5.

$$z_1 > y_1-1.$$

PROOF. First, the functions α, β, and γ as defined in Lemma 2.4.1 are estimated. Lemmas 7.2.4, 7.4.2, and 7.4.4 yield for $k \in [y_0+1,1,y_1-1]$:

$$\alpha(k) = (A(k) - B(k))F(k)G(k) \leq .1434\omega^4 k \frac{\sin^2(\omega_1(k-y_0))}{\sin^2\omega_1} .$$

Since

$$\frac{\sin \omega_1}{\omega_1} \geq 1 - \frac{1}{6}\omega_1^2 \geq 1 - \frac{(.9607)^2}{24t^2} \geq .9996,$$

it follows that

$$\alpha(k) \leq .1434\omega^4 k \frac{\sin^2(\omega_1(k-y_0))}{(.9996)^2\omega_1^2} \leq \frac{.1436\omega^2 k}{(.9607)^2} \sin^2(\omega_1(k-y_0)) \leq$$

$$\leq .1556\omega^2 k \sin^2(\omega_1(k-y_0)).$$

For $k \in [y_0+1,1,y_1-1]$, one has by Lemmas 2.2.4, 7.4.1, and 7.4.2:

$$\beta(k) = \sum_{i\in[y_0+1,1,k)} \alpha(i) \leq .1556\omega^2 \sum_{i\in[y_0+1,1,k)} i \sin^2(\omega_1(i-y_0)) =$$

$$= .1556\omega^2 \sum_{j=1}^{k-y_0-1} (y_0+j)\sin^2(\omega_1 j) \leq .1556\omega^2(\tfrac{1}{2}y_0\lceil\tfrac{\pi}{\omega_1}\rceil + \tfrac{1}{4}\lceil\tfrac{\pi}{\omega_1}\rceil^2) \leq$$

$$\leq .1556\omega^2(\tfrac{1}{2}\frac{1.7101}{\omega}(\frac{3.2702}{\omega} + \frac{1}{2\omega t}) + \tfrac{1}{4}(\frac{3.2702}{\omega} + \frac{1}{2\omega t})^2) \leq .8706.$$

For $k \in [y_0+1,1,\eta]$, the following estimate is better (cf. Lemma 2.2.2):

$$\beta(k) \leq .1556\omega^2\omega_1^2 \sum_{j=1}^{k-y_0-1} (y_0+j)j^2 \leq$$

$$\leq .1556(.9607)^2\omega^4(\frac{1}{3}y_0(k-y_0)^2(k-y_0-1) + \frac{1}{4}(k-y_0)^3(k-y_0-1)) \leq$$

$$\leq .0120\omega^4(k-y_0)^2(k-y_0-1)(3k+y_0).$$

Hence, by Lemma 7.4.3 one has for $k \in [y_0+1,1,\eta]$:

$$\gamma(k) = \sum_{i\in(y_0+1,1,k]} \frac{\beta(i)}{F(i)F(i-1)} \leq$$

$$\leq \frac{.0120\omega^4}{(.5844)^2} \sum_{i\in(y_0+1,1,\eta]} \frac{(i-y_0)^2(i-y_0-1)(3i+y_0)}{(i-y_0)(i-y_0-1)} \leq$$

$$\leq .0352\omega^4 \sum_{j=2}^{\eta-y_0} j(4y_0+3j) \leq$$

$$\leq .0352\omega^4(2y_0(\eta-y_0)(\eta-y_0+1) + (\eta-y_0)(\eta-y_0+1)^2) =$$

$$= .0352\omega^4(\eta-y_0)(\eta-y_0+1)(\eta+y_0+1) \leq$$

$$\leq .0352\ \frac{1.6851}{2t}(1.6851 + \frac{1}{2t})(1.6851 + 2\cdot 1.7101 + \frac{1}{2t}) \leq .0266$$

(cf. Lemma 7.4.1). For $k \in [\eta,1,y_1-1]$ one has by Lemmas 7.4.3 and 2.2.5:

$$\gamma(k) - \gamma(\eta) = \sum_{i\in(\eta,1,k]} \frac{\beta(i)}{F(i)F(i-1)} \leq$$

$$\leq \frac{.8706}{(.9847)^2}\,\omega^2 \sum_{i\in(\eta,1,y_1-1]} \frac{1}{\sin(\omega_1(y_1-i))\sin(\omega_1(y_1-i+1))} \leq$$

$$\leq .8979\omega^2 \sum_{j=2}^{y_1-\eta} \frac{1}{\sin(\omega_1 j)\sin(\omega_1(j-1))} \leq .8979\,\frac{\omega^2}{\omega_1^2} = \frac{.8979}{(.9607)^2} \leq$$

$$\leq .9729.$$

Hence, for $k \in [y_0+1,1,y_1-1]$:

$$\gamma(k) \leq .0266 + .9729 = .9995.$$

Now Lemma 2.4.1 establishes that

$$G(k) \geq .0005\ F(k) > 0$$

for $k \in [y_0+1,1,y_1-1]$. Hence $z_1 > y_1-1$, proving the lemma. □

The assertions $y_1-y_0 \in \mathbb{Z}$ (Lemma 7.4.2), $z_1-y_0 \in \mathbb{Z}$ (Lemma 7.4.4), $z_1 < y_1$ (Lemma 7.4.4), and $z_1 > y_1-1$ (Lemma 7.4.5) are clearly contradictory. This proves

LEMMA 7.4.6. *The assumptions made in this chapter are inconsistent.*

CHAPTER 8

SHORT-WAVE KRAVČUK POLYNOMIALS

In the previous two chapters, it was supposed that $\omega \leq 1/(2t)$. In the present chapter, the nonexistence of perfect codes for which $\omega > 1/(2t)$ will be proved.

In this entire chapter, it is assumed that $\omega > 1/(2t)$.

Recall that the assumptions stated in Section 5.5 still hold. In particular the polynomial K_t is assumed to have integral zeros.

8.1. Some inequalities involving n, q, and t

In this section, some inequalities are established which will be used in the subsequent sections to disprove the existence of any perfect code satisfying $\omega > 1/(2t)$. Define m by

$$m = n-t+1.$$

The observation in the next lemma is crucial.

LEMMA 8.1.1.

$$q^j \mid \binom{t}{j} m^{(j)} \quad \textit{for all } j \in [0,1,t].$$

PROOF. Define P by

$$P(w) = q^{-t} t!\, K_t(n-w).$$

By Lemma 3.1.2 it follows that

$$P(w) = q^{-t} t! \sum_{j=0}^{t} (-1)^{t-j} q^j \binom{n-j}{t-j} \binom{w}{j} = \sum_{j=0}^{t} \left(\frac{-1}{q}\right)^{t-j} \binom{t}{j} m^{(t-j)} w_{(j)}.$$

Defining c_j for $j \in [0,1,t]$ by

$$c_j = (\frac{-1}{q})^{t-j} \begin{bmatrix} t \\ j \end{bmatrix}_m^{(t-j)},$$

one has

$$P(w) = \sum_{j=0}^{t} c_j w_{(j)}.$$

It is obvious that $w_{(j)}$ can be expanded in powers of w:

$$w_{(j)} = \sum_{k=0}^{j} S_{j,k} w^k,$$

where the numbers $S_{j,k}$ are integers, and $S_{k,k} = 1$. (They are called the Stirling numbers of the first kind, cf. RIORDAN [23].) Now

$$P(w) = \sum_{j=0}^{t} c_j \sum_{k=0}^{j} S_{j,k} w^k = \sum_{k=0}^{t} a_k w^k,$$

where

$$a_k = \sum_{j=k}^{t} S_{j,k} c_j.$$

In particular, $a_t = c_t = 1$, so P is a monic polynomial. Since P has integral zeros, it must have integral coefficients:

$$a_k \in \mathbb{Z} \text{ for } k \in [0,1,t].$$

Since

$$c_k = a_k - \sum_{j=k+1}^{t} S_{j,k} c_j,$$

it is clear that

$$c_k \in \mathbb{Z} \text{ for } k \in [0,1,t].$$

Hence, by the definition of c_k:

$$q^{t-k} \mid \begin{bmatrix} t \\ k \end{bmatrix}_m^{(t-k)} \text{ for } k \in [0,1,t].$$

The lemma follows by replacing k by t-j. □

For j=1, the lemma yields:

COROLLARY. $q \mid tm$.

Next, the numbers $c_{j,k}$ for $j \in \mathbb{N}$, $k \in \mathbb{N}$, $k < j$ are defined recursively by

$$c_{j,0} = \frac{1}{j!}$$

$$c_{j,k} = (j-k)\operatorname{lcm}(c_{j,k-1}, c_{j-1,k-1}) \text{ if } k \neq 0.$$

Some values of $c_{j,k}$ are listed in Table 8.1.1.

j \ k	0	1	2	3	4	5
1	1	–	–	–	–	–
2	1/2	1	–	–	–	–
3	1/6	1	1	–	–	–
4	1/24	1/2	2	2	–	–
5	1/120	1/6	3/2	12	12	–
6	1/720	1/24	2/3	18	72	72

Table 8.1.1. The values of $c_{j,k}$ for $j \leq 6$.

Using the numbers $c_{j,k}$ defined above, the following consequence of Lemma 8.1.1 can be formulated.

LEMMA 8.1.2. *Let* $j \in \mathbb{N}$, $k \in \mathbb{N}$, $k < j$. *Then*

$$q^j \mid c_{j,k} t^k t_{(j)}{}^{m(j-k)}.$$

PROOF. For k = 0, the assertion is an immediate consequence of Lemma 8.1.1 and the definition of $c_{j,0}$.

Suppose that the assertion has been proved for k-1 instead of k. Then

$$q^j \mid c_{j,k-1} t^{k-1} t_{(j)}{}^{m(j-k+1)},$$

and

$$q^{j-1} \mid c_{j-1,k-1} t^{k-1} t_{(j-1)}{}^{m(j-k)}.$$

Since

$$1 \Big| \frac{c_{j,k} t}{(j-k) c_{j,k-1}},$$

the first relation yields

$$q^{j} \Big| \frac{c_{j,k} t^{k} t_{(j)}{}^{m(j-k+1)}}{j-k}.$$

Since

$$q \Big| \frac{c_{j,k} t(t-j+1)m}{(j-k) c_{j-1,k-1}}$$

(recall that $q \mid tm$), the second relation yields

$$q^{j} \Big| \frac{c_{j,k} t^{k} t_{(j)}{}^{m(j-k)_m}}{j-k}.$$

Hence

$$q^{j} \Big| \frac{c_{j,k} t^{k} t_{(j)}{}^{m(j-k+1)}}{j-k} - \frac{c_{j,k} t^{k} t_{(j)}{}^{m(j-k)_m}}{j-k} = c_{j,k} t^{k} t_{(j)}{}^{m(j-k)},$$

which completes the proof of the lemma by induction. □

Lemma 8.1.2 will be applied only with j=6 and k=5.

COROLLARY $q^{6} \mid 72 t^{5} t_{(6)}{}^{m}$.

For each prime power p^{α}, the number λ is defined by

$$\lambda = p^{\alpha-1/(p-1)}.$$

Some values of λ are listed in Table 8.1.2.

p^α	2	3	4	5	7	8	9	11	13	16
λ	1	1.73	2	3.34	5.06	4	5.20	8.65	10.50	8

Table 8.1.2. The values of λ (rounded to two decimal places) for $p^\alpha \leq 16$.

Now the following lemma can be formulated.

LEMMA 8.1.3. *Let* p^α *be a prime power dividing* q. *Then*

$$n \geq \left(\frac{q}{q-1}\right)^{1.2\lambda t}.$$

PROOF. Lemma 8.1.1 with j=t yields:

$$q^t \mid m^{(t)}.$$

Since $p^\alpha \mid q$, and $m = n-t+1$,

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

Let ν be a number amongst n,n-1,...,n-t+1 which contains the maximum number of factors p. Then

$$p^{\alpha t - (\lfloor (t-1)/p \rfloor + \lfloor (t-1)/p^2 \rfloor + \ldots)} \mid \nu,$$

so

$$n \geq \nu \geq p^{\alpha t-(t-1)/(p-1)} = \lambda^t p^{1/(p-1)}.$$

It can be checked easily that $p^{1/(p-1)} \geq q^{1/(q-1)} \geq \left(\frac{q}{q-1}\right)^{1.2}$ for $q \geq 3$. □

Combination of the various estimates yields the following general result, in which n does not occur anymore.

LEMMA 8.1.4. *Let* p^α *be a prime power dividing* q. *Then*

$$\lambda \leq (13t^{5.8})^{1/t}.$$

PROOF. From the assumption $\omega > 1/(2t)$, it is known that

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

so by the corollary to Lemma 8.1.2:

$$n^6 < (\frac{2qt^2(2t+1)}{q-1})^6 72t^5 t_{(6)}^n =$$

$$= (\frac{4q}{q-1})^6 \ 72nt^{18}(t-1)(t-2)(t-3)(t-4)(t-5)(t+\tfrac{1}{2})^6 \le (\frac{4q}{q-1})^6 \ 72nt^{29} .$$

Hence

$$n \le (\frac{4q}{q-1})^{1.2} \ 72^{\cdot 2}t^{5.8} .$$

Combination with Lemma 8.1.3 yields

$$\lambda^t \le 4^{1.2} \ 72^{\cdot 2}t^{5.8} \le 13t^{5.8} . \ \square$$

8.2. The prime divisors of q

In this section it is proved that q can only contain a very limited number of prime divisors.

LEMMA 8.2.1. $q \mid 2520$.

PROOF. The upper bound for λ in Lemma 8.1.4 is monotonically decreasing in t for $t \ge 7$. Hence

$$\lambda \le (13 \cdot 7^{5.8})^{1/7} < 8 .$$

From Table 8.1.2 it follows that $p^\alpha \in \{2,3,4,5,7,8,9\}$. (Observe that $\lambda = p^{\alpha - 1/(p-1)} \ge \frac{1}{2} p^\alpha \ge 8$ for $p^\alpha \ge 16$.) Hence $q \mid 5 \cdot 7 \cdot 8 \cdot 9 = 2520$. $\square$

LEMMA 8.2.2. *If* $t \ge 10$, *then* $q \mid 120$.

PROOF. For $t \ge 10$ it follows that

$$\lambda \le (13 \cdot 10^{5.8})^{1/10} < 5 .$$

Hence $p^{\alpha} \in \{2,3,4,5,8\}$, and consequently $q \mid 3\cdot5\cdot8 = 120$. □

Together with H. Laakso's result, this yields the impossibility of $t \geq 10$.

LEMMA 8.2.3. $t < 10$.

PROOF. Immediate from Lemmas 4.4.3 and 8.2.2.

The remaining cases $t = 7$ and $t = 9$ will be treated in the next section.

8.3. The cases $t = 7$ and $t = 9$

LEMMA 8.3.1. $t \neq 7$.

PROOF. From Lemmas 8.2.1 and 4.4.3 it follows that $q = 2^{\alpha}\cdot3^{\beta}\cdot5\cdot7$ with $\alpha \in \{1,2,3\}$ and $\beta \in \{1,2\}$.

Suppose that $t = 7$. Then the assumption $\omega > 1/(2t)$ yields

$$m \leq n \leq \frac{1470q^2}{q-1} .$$

Lemma 8.1.1 gives e.g.

$$q \mid 7m,$$

$$q^2 \mid 21m(m+1),$$

$$q^3 \mid 35m(m+1)(m+2),$$

$$q^4 \mid 35m(m+1)(m+2)(m+3),$$

$$q^7 \mid m(m+1)(m+2)(m+3)(m+4)(m+5)(m+6)..$$

It follows from the first, second, fourth, and last of the above relations respectively that $2 \mid m$, $4 \mid m$, $8 \mid m$, and finally

$$2^{7\alpha-4} \mid m.$$

In the same way it follows that

$$3^{7\beta-2} \mid m,$$

and

$$5^6 \mid m.$$

Hence,

$$\frac{q^7}{720 \cdot 7^7} = 2^{7\alpha-4} \cdot 3^{7\beta-2} \cdot 5^6 \mid m \leq \frac{1470q^2}{q-1},$$

so $q \leq 97$. This contradicts $q \geq 2 \cdot 3 \cdot 5 \cdot 7 = 210$. □

LEMMA 8.3.2. $t \neq 9$.

PROOF. Suppose that $t = 9$. Then

$$m \leq n \leq \frac{3078q^2}{q-1}.$$

Lemma 8.1.1. gives e.g.

$$q \mid 9m,$$

$$q^2 \mid 36m(m+1),$$

$$q^9 \mid m(m+1)(m+2)(m+3)(m+4)(m+5)(m+6)(m+7)(m+8).$$

Because of Lemmas 8.2.1 and 4.4.3, q should be divisible by 7. Hence,

$$5764801 = 7^8 \mid m \leq \frac{3078q^2}{q-1},$$

so $q \geq 1872$. This implies that $q = 2520$ (cf.Lemma 8.2.1).

Since $9 \mid q$, it follows that $3^{16} \mid m$ or $3^{16} \mid m + 1$. Hence

$$43046720 = 3^{16}-1 \leq m \leq \frac{3078q^2}{q-1} \leq 7759640,$$

which is false. □

CHAPTER 9

CONCLUSION AND DISCUSSION

In Chapters 6 and 7, it was proved that t-perfect q-ary codes of length n+1 cannot exist provided $q \geq 3$, $t \geq 7$, $t \neq 8$, $t \leq n$, and $\omega \leq 1/(2t)$.

In Chapter 8, the same was proved provided $q \geq 3$, $t \geq 7$, $t \neq 8$, $t \leq n$, and $\omega > 1/(2t)$.

Combination of these results with the Lemmas 4.4.1 and 4.4.2 establishes the conclusion of this thesis.

THEOREM. *The only nondegenerate* t*-perfect codes with* $t \geq 3$, $t \neq 6$, and $t \neq 8$ *are the* 3*-perfect binary Golay code of length* 23, *and the* t*-perfect binary repetition codes of length* 2t+1 *(for any* $t \geq 3$*).*

The theorem does not give a decisive answer to the existence of 1-, 2-, 6-, or 8-perfect codes. Indeed, the method applied is absolutely worthless for single or double error correcting codes, since the corresponding Kravčuk polynomials do not have enough zeros. Furthermore, Lloyd's theorem is very weak when applied to these codes. They require a totally different, still unknown, approach.

For 6- and 8-perfect codes, the method could work in principle, although they require special treatment. According to numerical data, Lemma 7.4.5 still holds for t = 8. We are convinced that it must be possible to prove it by sharpening the bounds. Presumbly, one must replace the approximation by ordinary sine functions by 8-th degree Hermite polynomials, as was done by E. BANNAI [1].

For 6-perfect codes, the problem is more difficult, since numerical data show that Lemma 7.4.5 is false for t=6. Presumably, $y_1-2 < z_1 < y_1-1$ is true instead. This will be much harder to prove, though probably still feasible. On the other hand, it might also be possible to generalize the method of REUVERS [22] to t=6 or even to t=8.

Finally, it can be added that the results in Chapter 8 can easily be

extended to t=6 or t=8.

REFERENCES

[1] BANNAI, E., *On perfect codes in the Hamming schemes* H(n,q) *with* q *arbitrary*, J. Combinatorial Theory (A) 23 (1977) 52-67.

[2] BASSALYGO, L.A., V.A. ZINOV'EV, V.K. LEONT'EV & N.I. FEL'DMAN, *Nonexistence of perfect codes over some alphabets*. Problemy Peredači Informaticii 11 (1975) 3-13.

[3] BEST, M.R., *Optimal Codes*, Chapter 9 in "Packing and covering in combinatorics" (A. Schrijver, ed.), Amsterdam, Mathematical Centre, 1979. Mathematical Centre Tracts, nr. 106.

[4] BEST, M.R., *On the existence of perfect codes*, Mathematical Centre Report ZN 82/78, Math. Centre, Amsterdam, 1978.

[5] DELSARTE, P., *Bounds for unrestricted codes, by linear programming*, Philips Research Reports, 27 (1972) 289-296.

[6] DELSARTE, P. & J.-M. GOETHALS, *Unrestricted codes with the Golay parameters are unique*, Discrete Mathematics 12 (1975) 211-224.

[7] GOLAY, M.J.E., *Notes on digital coding*, Proc. IRE 37 (1949) 657.

[8] HAMMING, R.W., *Error detecting and error correcting codes*, Bell Syst. Tech. J., 29 (1950) 147-160.

[9] LAAKSO, H., *Nonexistence of nontrivial perfect codes in the case* $q = p_1^a p_2^b p_3^c$, $e \geq 3$, Ann. Univ. Turku, Ser. A.I, (1979), nr. 177.

[10] LENSTRA, H.W., jr., *Two theorems on perfect codes*, Discrete Mathematics, 3 (1972) 125-132.

[11] LINSTRÖM, B., *On group and nongroup perfect codes in q symbols*, Math. Scand., 25 (1969) 149-158.

[12] LINT, J.H. VAN, *On the nonexistence of perfect* 2- *and* 3-*error correcting codes over* GF(q), Information and Control, 16 (1970) 396-401.

[13] LINT, J.H. VAN, *On the nonexistence of perfect 5-, 6- and 7- error correcting codes over* GF(q), Eindhoven, The Netherlands; Technological University Eindhoven, 1970. Report 70-WSK-06.

[14] LINT, J.H. VAN, *On the nonexistence of certain perfect codes*, Computers in Number Theory. London-New York, Academic Press, 1971; 277-282.

[15] LINT, J.H. VAN, *Nonexistence theorems for perfect error correcting codes*, in "Computers in Algebra and Number Theory", Providence, American Mathematical Society, 1971. SIAM-AMS Proceedings, vol. 4, 89-95.

[16] LINT, J.H. VAN, *Coding Theory*, Berlin etc., Springer Verlag, 1973. Lecture Notes in Mathematics, vol. 201.

[17] LINT, J.H. VAN, *Recent results in perfect codes and related topics*, in "Combinatorics" (M. Hall & J.H. van Lint eds.), Amsterdam, Mathematical Centre, 1974. Mathematical Centre Tracts, nr. 55, 163-183.

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

[19] MACWILLIAMS, F.J., *A theorem on the distribution of weights in a systematic code*, Bell Syst. Tech. J., 42 (1963) 79-94.

[20] MACWILLIAMS, F.J. & N.J.A. SLOANE, *The theory of error correcting codes*, Amsterdam, North Holland Publ. Comp., 1977.

[21] POLYA, G. & G. SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis*, Vol. 2, 2nd ed., Berlin, Springer Verlag, 1964.

[22] REUVERS, H.F.H., *Some nonexistence proofs for perfect codes over arbitrary alphabets*, Ph.D. Thesis, Technological University Eindhoven, 1977.

[23] RIORDAN, J., *An introduction to combinatorial analysis*, New York, Wiley, 1958.

[24] SCHÖNHEIM, J., *On linear and nonlinear single-error-correcting q-nary perfect codes*, Information and Control, 12 (1968) 23-26.

[25] SNOVER, S.L., *The uniqueness of the Nordstrom-Robinson and the Golay binary codes*, Ph. D. Thesis, Dept. of Mathematics, Michigan State University, 1973.

[26] SZEGÖ, G., *Orthogonal Polynomials*, Colloquium Publications, Vol. 23, New York, Amer. Math. Soc., revised edition, 1959.

[27] TIETÄVÄINEN, A., *On the nonexistence of perfect 4-Hamming-error-correcting codes*, Ann. Acad. Scient. Fennicae, ser. A.I, (1970), nr. 485.

[28] TIETÄVÄINEN, A., *A short proof for the nonexistence of unknown perfect codes over* GF(q), q > 2, Ann. Acad. Scient. Fennicae, ser. A.I, (1974), nr. 580.

[29] TIETÄVÄINEN, A., *Nonexistence of nontrivial perfect codes in case* $q = p_1^s p_2^t$, e ≥ 3, Discrete Mathematics, 17 (1977) 199-205.

[30] TIETÄVÄINEN, A. & A. PERKO, *There are no unknown perfect binary codes*, Ann. Univ. Turku, Ser. A.I, (1971), nr. 148.

[31] VASIL'EV, J.L., *On nongroup close-packed codes* (In Russian), Probl. Kibernet., 8 (1962) 337-339, translated in Probleme der Kybernetik, 8 (1965) 375-378.

[32] WHITTAKER, E.T. & G.N. WATSON, *A course of modern analysis*, Cambridge Univ. Press, 4th ed., 1963.

[33] GANTER, B., F. HERGERT & H. BAUER, *Some new-perfect codes*, presented at the meeting on finite geometries, Oberwolfach, March 22-26, 1982.

SAMENVATTING

Dit proefschrift bestaat in feite uit één stelling met het daarbij behorende bewijs. Deze stelling zegt dat er geen onbekende t-perfecte codes over willekeurige alfabetten bestaan, tenzij t gelijk is een 1, 2, 6, of 8.

Het bewijs berust op de stelling van Lloyd, en maakt geen gebruik van de bolpakkingsvoorwaarde. De voor Kravčuk polynomen geldende differentievergelijking wordt gebruikt om aan te tonen dat - onder zekere voorwaarden - de middelste drie of vier nulpunten van dit soort polynomen niet gelijktijdig geheel kunnen zijn. Dit bewijst het niet-bestaan van onbekende perfecte codes met een relatief grote bloklengte.

Het bestaan van perfecte codes met een relatief kleine bloklengte wordt uitgesloten door een stelsel deelbaarheidsrelaties af te leiden, dat gelijkwaardig is met de geheeltalligheid van de som, het product, etc. van de nulpunten van een Kravčuk polynoom.

De bewijsmethode kan vermoedelijk worden gegeneraliseerd tot t = 6 en t = 8, maar is niet toepasbaar voor t = 1 of t = 2.

STELLINGEN

bij het proefschrift

A CONTRIBUTION TO THE NONEXISTENCE OF PERFECT CODES

van

M.R. Best

2 juni 1982

1. Het is niet zinvol een wiskundige stelling (theorema) als stelling (these) bij een proefschrift te voegen, aan gezien een wiskundige stelling niet discutabel is, en een these dit wel behoort te zijn.

2. Met behulp van Lemma 8.1.1 uit dit proefschrift kunnen vele bekende bewijzen van het niet-bestaan van klassen van perfecte en gelijkmatig verdeelde codes aanmerkelijk vereenvoudigd worden.

3. Zij d de minimum afstand van een niet-ontaarde, niet-repetitie code, en s' de uitwendige afstand. Dan geldt vermoedelijk:

$$s' \geq d - 4.$$

Verder bestaan codes met s' gelijk aan d-4, d-3, d-2, en wellicht ook d-1 slechts in beperkte mate. Dit soort reguliere codes generaliseren perfecte en gelijkmatig verdeelde codes, zonder triviaal te worden voor kleine waarden van d.

4. Een [n,M,d]-code is een binaire code met bloklengte n en minimum afstand d die M codewoorden bevat. Zo een code heet *optimaal* als er geen [n,M',d]-code bestaat met M' > M.
Vermoedelijk gelden de volgende uitspraken:
   - er bestaat een [18,72,8]-code;
   - de [11,72,4]-(JULIN) code is optimaal;
   - de [19,128,8]-code is optimaal (d.w.z. de vijf keer ingekorte GOLAY code is optimaal);
   - een optimale [n,M,d]-code met $n \equiv d \pmod 2$ en $n \geq 2d$ blijft na één keer inkorten optimaal.

5. Er bestaat een sterke analogie tussen de exactheid van de wiskunde van vóór CAUCHY, en de exactheid van de wiskundige notatie van tegenwoordig. De "het - staat - er - wel - niet - maar - je - begrijpt - toch - wat - ik - bedoel" - mentaliteit is onwiskundig en gevaarlijk.

6. In veel notaties wordt de fout gemaakt dat met een expressie wordt getracht informatie over te brengen. Dit komt vooral tot uiting in het "fysische" functiebegrip, waarin "V(P,T)" zou betekenen dat V van P en T afhangt. Uitdrukkingen als "$\delta = \delta(\varepsilon)$" zijn in serieuze wiskundige literatuur ten ene male verwerpelijk.

7. Het is opmerkelijk dat iemand wel bezwaar heeft tegen de notatie "$A \Rightarrow B \Rightarrow C$" als ordeningsrelatie tussen drie logische expressies, maar geen bezwaar heeft tegen, en zelf ook veelvuldig gebruik maakt van, de notatie "$a \leq b \leq c$" voor een ordeningsrelatie tussen drie arithmetische expressies. Overigens zijn beide notaties volledig te rechtvaardigen.

   H.C.A. VAN TILBORG, *Uniformly packed codes*, Proefschrift Technische Hogeschool Eindhoven, 1976 (Stelling IX).

8. Het is merkwaardig dat naast de begrippen "verzameling", "geordende verzameling", en "rij" (= functie op een geordende verzameling), het hier logisch bijpassende begrip "functie op een verzameling" geen standaardbenaming heeft. De begrippen "familie", "tupel", en het vreselijke "verzameling met herhaling" dekken alle ongeveer dezelfde lading, maar zijn geen van drieën algemeen geaccepteerd.

9. In tegenstelling tot wat de meeste leerboeken beweren, is een stochastische variabele een variabele, en (i.h.a.) geen functie.

10. De rol van de letter "d" in de meest gangbare notaties voor een integraal t.o.v. een maat μ ("$\int f(x)d\mu(x)$" en "$\int f(x)\mu(dx)$") is duister. De juiste notatie is "$\int f(x)\mu(x)$". Men vergelijke: J.-P. SERRE, *A course in arithmetic*, Springer, New York, 1973, p.65 of p.106.

11. De angst, veelal verborgen in een onterecht misprijzen, die de meeste wiskundigen hebben voor de lege verzameling (de lege functie, het getal 0, etc.) is beangstigend.

12. Een niet onbelangrijk aspect van het gestructureerd programmeren is dat de layout van het voor de menselijke lezer bestemde programma duidelijk en consequent is. Het onder elkaar plaatsen van bij elkaar behorende "begin"-s en "end"-s hoeft hier echter niet toe bij te dragen, en is in zeker opzicht zelfs ongewenst. Dit gebruik wordt zonder meer lachwekkend indien het leidt toe regels met één enkel sluithaakje.

13. De meest efficiënte methode om een FORTRAN programma te schrijven, is het eerst te ontwikkelen in een hogere programmeertaal, en het op het allerlaatst te converteren naar FORTRAN. Het nut van deze laatste exercitie is twijfelachtig.

14. Er is geen enkele reden om aan te nemen dat de raaklijnen in de singulariteit die optreedt in het P-x-diagram van een twee-componenten-, twee-fasenevenwicht waarvoor gas-gasevenwicht bestaat (het z.g. "kritische dubbelpunt") zouden samenvallen.

    J.A. SCHOUTEN, *Vloeistof-gas- en gas-gasevenwichten in de systemen neon-argon en neon-krypton*, Proefschrift Universiteit van Amsterdam, 1969.

15. Er bestaat een eenvoudige vuistregel, met betrekkelijk weinig uitzonderingen, hoe de electronen in een atoom over de verschillende energieniveaus zijn verdeeld. De gangbare methoden om de elementen in het periodiek systeem te rangschikken zijn hiermee niet in overeenstemming.

16. Er bestaat een methode om twee kruisende autosnelwegen op elkaar aan te sluiten die de bezwaren van een klaverblad ondervangt, en die bovendien minder viaduct-oppervlak vereist.

17. Het is onterecht dat men in Nederland wel de vrijheid heeft om op principiële gronden te weigeren voor andermans vrijheid en veiligheid op te komen, maar niet om te weigeren voor zijn eigen veiligheid op te komen.

18. Het is aanzienlijk eenvoudiger het jaar 0 achteraf alsnog in te voeren, en alle jaartallen van vóór Christus (in absolute waarde) met één te verlagen, dan de mensheid, en i.h.b. de pers, aan het verstand te brengen dat het volgende decennium niet op 1 januari 1990, en de volgende eeuw niet op 1 januari 2000 begint. Met het eerste alternatief zou een - alleszins verklaarbare - historische blunder worden rechtgezet.

19. Het is uitermate onlogisch dat in het bridgespel een bod van meer dan dertien slagen niet (meer) is toegestaan.