New asymptotic bounds for self-dual codes and lattices

Eric M. Rains

AT&T Research

rains@research.att.com

April 12, 2001

Abstract

We give an independent proof of the Krasikov-Litsyn bound $d/n \lesssim (1-5^{-1/4})/2$ on doubly-even self-dual binary codes. The technique used (a refinement of the Mallows-Odlyzko-Sloane approach) extends easily to other families of self-dual codes, modular lattices, and quantum codes; in particular, we show that the Krasikov-Litsyn bound applies to singly-even binary codes, and obtain an analogous bound for unimodular lattices. We also show that in each case, our bound differs from the true optimum by an amount growing faster than $O(\sqrt{n})$.

1 Introduction

In [10], [9], Mallows, Odlyzko, and Sloane proved the following result:

Theorem. *Let C be a doubly-even binary self-dual code of length n and minimum distance d. Then $d \leq 4[n/24] + 4$. Morever, for any constant b, one has $d \leq n/6 - b$ for sufficiently large n.*

as well as analogous results for ternary codes and even unimodular lattices. The first claim has since been extended to singly-even binary self-dual codes [15], and analogous results have been obtained for even strongly modular lattices [12], [13] and odd strongly modular lattices [19], including the odd unimodular case.

Regarding the asymptotic claim, essentially the only improvement is the bound of Krasikov and Litsyn [7]:

Theorem. *Let C_i be a family of doubly-even binary self-dual codes of length tending to infinity. Then*

$$\limsup_{i\to\infty} \frac{d(C_i)}{n(C_i)} \leq \frac{1 - 5^{-1/4}}{2}. \tag{1.1}$$

However, it is unclear to what extent their argument extends to the other cases of interest (especially the lattice cases).

In the present paper, we give a new technique for deriving bounds on self-dual codes and modular lattices. In the doubly-even binary case, our bound is precisely the Krasikov-Litsyn bound; the difference is that our technique easily generalizes. The basic idea (following [9]) is to use invariant theory to construct linear relations

that must be satisfied by the weight enumerator of a self-dual code. In the doubly-even binary case, the simplest such relation gives $d \leq 4[n/24] + 4$; to obtain their asymptotic improvement, Mallows, Odlyzko, and Sloane also take into account the second-simplest relation. Somewhat surprisingly, our bounds also only use these two relations; equivalently, we only consider the coefficients of the weight enumerator up to weight $4[n/24] + 8$.

To compute the coefficients of these relations, we use the Bürmann-Lagrange theorem to express them as coefficients of certain power series, which we asymptotically analyze via Cauchy's integral and the saddle-point method. Under suitable conditions on the power series, we can then show that their coefficients in certain ranges are asymptotically uniformly positive, and thus give a contradiction unless the minimum distance bound holds. This necessitates a certain amount of analysis, which we deal with in Section 2. Then, in Section 3, we give our main theorem, Theorem 3.6. This is stated in some generality (regarding the minimum valuations of certain families of power series with nonnegative coefficients), so as to include most of our applications as special cases. We state these special cases in Section 4; see Theorem 4.1 for (most) codes, Theorem 4.2 for even modular lattices, and Theorems 4.3 and 4.5 for codes over $\mathbb{Z}_4$. The remaining applications not directly dealt with by Theorem 3.6 are considered in Section 5; see Theorem 5.1 for (singly-even) self-dual binary codes, Theorem 5.2 for odd modular lattices, and Theorems 5.5 and 5.6 for quantum codes.

As we remarked, our improvements on the main Mallows-Odlyzko-Sloane bounds are obtained by considering the first two relations coming from invariant theory, rather than just the first. In Section 6, we consider the possibility of improving the bounds by using the first k relations. In fact, it turns out that, despite the significant improvement between $k = 1$ and $k = 2$, increasing k beyond 2 does not give a better bound on $\limsup d/n$. We do, however, obtain a slight lower-order improvement (Theorem 6.1); increasing k gives an $O(n^{-1/2})$ improvement on the bound on d/n. In particular, each of our bounds differs from the true optimal minimum distance (norm) by an amount growing faster than $O(\sqrt{n})$.

2 Lemmas

We will use the notation $[t^j]f(t)$ to refer to the coefficient of t^j in the (formal) Laurent series $f(t)$. We also use the notation

$$f \succeq g \tag{2.1}$$

to say that $[t^j](f(t) - g(t)) \geq 0$ for all j.

Lemma 2.1. *Let $f(t)$ be a Laurent series convergent on an annulus $0 \leq r_1 < |t| < r_2 \leq \infty$. If $f \succeq 0$, then we have the bound*

$$|f(t)| \leq f(|t|) \tag{2.2}$$

valid on the annulus. If $[t^j]f(t)$ and $[t^{j+1}]f(t)$ are both nonzero for some j, then equality can hold only when $t = |t|$.

Proof. We have:

$$|f(t)| = |\sum_j f_j t^j| \leq \sum_j f_j |t|^j = f(|t|), \tag{2.3}$$

with equality only when there exists α such that $t^j = \alpha|t|^j$ for all j with f_j nonzero. Dividing two consecutive such equations, we obtain $t = |t|$ as required. $\square$

The Hadamard three-circles theorem then immediately implies that $\log(f(e^s))$ is strictly convex, for $r_1 < e^s < r_2$. In fact, we have the slightly stronger statement:

Lemma 2.2. *let $f(t)$ be a Laurent series convergent on an annulus $0 \leq r_1 < |t| < r_2 \leq \infty$, and not proportional to z^n for any n. If $f \succeq 0$, then for $r_1 < e^s < r_2$,*

$$\frac{d^2}{ds^2} \log(f(e^s)) > 0. \tag{2.4}$$

Proof. Setting $r = e^s$, we have:

$$\frac{d^2}{ds^2} \log(f(e^s)) = \left(r\frac{d}{dr}\right)^2 \log(f(r)) = \frac{\left(r\frac{d}{dr}\right)^2 f(r)}{f(r)} - \left(\frac{r\frac{d}{dr} f(r)}{f(r)}\right). \tag{2.5}$$

Now, $f(r)$ is positive on $r_1 < r < r_2$, so we may freely multiply by $f(r)^2$; we thus need to show that

$$f(r) \left(r\frac{d}{dr}\right)^2 f(r) - \left(r\frac{d}{dr} f(r)\right)^2 > 0. \tag{2.6}$$

Now, the left-hand-side has a Laurent series convergent in the original annulus, namely

$$(\sum_j f_j t^j)(\sum_k k^2 f_k t^k) - (\sum_j j f_j t^j)(\sum_k k f_k t^k) = \sum_j \sum_k k^2 f_j f_k t^{j+k} - \sum_j \sum_k jk f_j f_k t^{j+k} \tag{2.7}$$

$$= \sum_j \sum_k \frac{(j-k)^2}{2} f_j f_k t^{j+k}. \tag{2.8}$$

Since this $\succeq 0$, and has at least one nonzero coefficient, the desired inequality follows. $\square$

Lemma 2.3. *Let F, G be real power series both convergent in the circle $|t| < r_0$. Suppose furthermore that $G \succeq 0$, with both $G(0)$ and $G'(0)$ positive. Then for any compact subset $I \subset [0, r_0)$ on which F is positive, and for all sufficiently large n (depending on I):*

$$[t^m]F(t)G(t)^n > 0 \tag{2.9}$$

whenever $m/n \in S(I)$, with $S(t) := tG'(t)/G(t)$.

Proof. It will suffice to show that

$$[t^{S(r)n}]F(t)G(t)^n = (F(r) + o(1))[t^{S(r)n}]G(t)^n, \tag{2.10}$$

3

with error uniform on any interval $r \in [0, a]$ with $a < r_0$, since then on I, $F(r)$ is bounded away from 0, while the error converges uniformly to 0. We split into two cases: $0 \le r \le n^{-2/3}$ and $n^{-2/3} \le r \le a$.

In the first region, we claim that for all sufficiently large n, and for $0 \le r \le n^{-2/3}$,

$$[t^{S(r)n}]F(t)G(t)^n = (F(0) + O(n^{-1/3}))G(0)^n \frac{(nS'(0))^{S(r)n}}{(S(r)n)!} \tag{2.11}$$

with error uniform in r. By Cauchy's residue theorem,

$$G(0)^{-n}[t^{S(r)n}]F(t)G(t)^n = \frac{1}{2\pi i} \int_{|t|=S(r)/S'(0)} t^{-S(r)n} F(t) \left(\frac{G(t)}{G(0)} \right)^n. \tag{2.12}$$

Now, $|t| = O(n^{-2/3})$, so we have the uniform estimates

$$\log G(t) - \log G(0) = S'(0)t + O(n^{-4/3}), \tag{2.13}$$

$$F(t) = F(0) + O(n^{-2/3}), \tag{2.14}$$

and thus

$$F(t) \left(\frac{G(t)}{G(0)} \right)^n = e^{S'(0)nt}(F(0) + O(n^{-1/3})). \tag{2.15}$$

Now,

$$\frac{1}{2\pi i} \int_{|t|=S(r)/S'(0)} t^{-S(r)n} F(0) e^{S'(0)nt} dt/t = F(0) \frac{(nS'(0))^{S(r)n}}{(S(r)n)!}, \tag{2.16}$$

so it remains to show that

$$(S(r)n)!(S'(0)n)^{-S(r)n} \frac{1}{2\pi i} \int_{|t|=S(r)/S'(0)} |\exp(S'(0)nt)| \frac{dt}{t} \tag{2.17}$$

is bounded. But, setting $m = S(r)n$ and rescaling t, this is

$$\frac{m!}{m^m} \frac{1}{2\pi i} \int_{|t|=1} e^{m \operatorname{Re}(t)} \frac{dt}{t} = \frac{m! I_0(m)}{m^m} = 1 + O(1/m), \tag{2.18}$$

by the known asymptotics of Bessel functions.

We now consider the case $n^{-2/3} \le r \le a$. Here, we claim

$$[t^{S(r)n}]F(t)G(t)^n = (2\pi n r S'(r))^{-1/2} r^{-S(r)n} G(r)^n (F(r) + O(n^{-1/60})), \tag{2.19}$$

again with uniform error. Again, Cauchy's integral gives

$$r^{S(r)n} G(r)^{-n}[t^{S(r)n}]F(t)G(t)^n = \frac{1}{2\pi} \int_{-\pi}^{\pi} e^{-iS(r)n\theta} F(re^{i\theta}) \left(\frac{G(re^{i\theta})}{G(r)} \right)^n d\theta. \tag{2.20}$$

Since

$$\frac{\log |G(re^{i\theta})| - \log G(r)}{r\theta^2} \tag{2.21}$$

4

is continuous and negative for $r \in [0, b]$, $\theta \in [-\pi, \pi]$, there exists a positive constant C such that

$$\log |G(re^{i\theta})| - \log G(r) \leq -Cr\theta^2 \qquad (2.22)$$

in that region.

In particular, when $|\theta| \geq n^{-9/20}r^{-1/2}$, we find $nr\theta^2 \geq n^{1/10}$, and thus

$$\left| \frac{G(re^{i\theta})}{G(r)} \right|^n \leq e^{-Cn^{1/10}}. \qquad (2.23)$$

Since $|F(re^{i\theta})|$ is bounded, we find that the contribution of this region to the integral is negligible.

Now, consider the region $|\theta| \leq n^{-9/20}r^{-1/2}$. Since

$$\frac{\log G(re^{i\theta}) - \log G(r) - iS(r)\theta + rS'(r)\frac{\theta^2}{2}}{r\theta^3} \qquad (2.24)$$

is continuous for $r \in [0, b]$, $\theta \in [-\pi, \pi]$, we find the uniform estimate

$$\log G(re^{i\theta}) - \log G(r) - iS(r)\theta + \frac{rS'(r)\theta^2}{2} = O(r\theta^3). \qquad (2.25)$$

or upon exponentiation,

$$e^{-iS(r)n\theta}G(r)^{-n}G(re^{i\theta})^n = e^{-nrS'(r)\theta^2/2}(1 + O(nr\theta^3)) = e^{-nrS'(r)\theta^2/2}(1 + O(n^{-1/60})), \qquad (2.26)$$

Similarly,

$$F(re^{i\theta}) = F(r) + O(n^{-7/60}), \qquad (2.27)$$

and thus

$$F(re^{i\theta})e^{-iS(r)n\theta}G(r)^{-n}G(re^{i\theta})^n = e^{-nrS'(r)\theta^2/2}(F(r) + O(n^{-1/60})). \qquad (2.28)$$

Since

$$\frac{1}{2\pi} \int_{|\theta| \leq n^{-9/20}r^{-1/2}} e^{-nrS'(r)\theta^2/2}d\theta = (2\pi nrS'(r))^{-1/2} + O(e^{-n^{1/10}S'(r)/2}), \qquad (2.29)$$

the claim follows. $\qquad \square$

Remark. Note that we only used the fact $G \succeq 0$ through the conclusions of the previous two lemmas.

Away from 0, we can give much stronger estimates (which will be used in the final section):

Lemma 2.4. *Fix radii $0 < r_1 < r_2 < \infty$, and let $F(t)$ and $G(t)$ be Laurent series convergent on a neighborhood of the annulus $r_1 \leq |t| \leq r_2$; suppose further that $G(t) \succeq 0$ and has two consecutive nonzero coefficients. Let $S(r) := rG'(r)/G(r)$, and for each $r_1 \leq r \leq r_2$, define a power series $\gamma(r, x)$ by $\gamma(r, 0) = 0$, $\gamma_x(r, 0) > 0$ and*

$$\log G(re^{i\gamma(r,x)}) = \log G(r) + iS(r)\gamma(r, x) - rS'(r)\frac{x^2}{2}. \qquad (2.30)$$

Then for all integers $k > 0$ and for $r_1 \leq r \leq r_2$, we have the asymptotic estimate

$$\sqrt{2\pi r S'(r)n} r^{S(r)n} G(r)^{-n} [t^{S(r)n}] F(t) G(t)^n = \sum_{0 \leq j \leq k-1} \frac{(rS'(r)n)^{-j}}{2^j j!} \left(\frac{d^{2j}}{dx^{2j}} \gamma_x(r,x) F(re^{i\gamma(r,x)}) \right)_{x=0} + O(n^{-k}),$$

(2.31)

with error uniform in r.

Proof. Note that

$$\log G(re^{iy}) = \log G(r) + iS(r)y - rS'(r)\frac{y^2}{2} + O(y^3);$$

(2.32)

since $rS'(r) > 0$, we conclude that $\gamma(r,x)$ converges for $|x| \leq x_0$ for some $x_0 > 0$ independent of r, and satisfies $\gamma_x(r,0) = 1$.

By Laurent's theorem,

$$\sqrt{2\pi r S'(r)n} r^{S(r)n} G(r)^{-n} [t^{S(r)n}] F(t) G(t)^n = \sqrt{\frac{rS'(r)n}{2\pi}} \int_{-\pi}^{\pi} F(re^{i\theta}) \left(\frac{e^{-iS(r)\theta} G(re^{i\theta})}{G(r)} \right)^n d\theta.$$

(2.33)

Now, as before, we can restrict the integral to any uniform neighborhood of 0, with exponentially small error. In particular, we may restrict to a neighborhood $|\theta| \leq \theta_0$ affording the change of variable $\theta = \gamma(r,x)$. The integral thus becomes

$$\frac{rS'(r)n}{2\pi} \int_{-x_0}^{x_0} \gamma_x(r,x) F(re^{i\gamma(r,x)}) e^{-nrS'(r)x^2/2} dx.$$

(2.34)

Now, we have the uniform estimate

$$\gamma_x(r,x) F(re^{i\gamma(r,x)}) = \sum_{0 \leq j \leq 2k-1} \frac{x^j}{j!} (\frac{d^j}{dx^j} \gamma_x(r,x) F(re^{i\gamma(r,x)}))_{x=0} + O(x^{2k});$$

(2.35)

since

$$\sqrt{rS'(r)n} 2\pi \int_{-x_0}^{x_0} x^{2k} e^{-nrS'(r)x^2/2} dx \leq \sqrt{rS'(r)n} 2\pi \int_{-\infty}^{\infty} x^{2k} e^{-nrS'(r)x^2/2} dx = (rS'(r)n)^{-k} \frac{(2k)!}{2^k k!},$$

(2.36)

the contribution of the error term is as required. Once we remove this term, the integral can be extended to ∞, again giving uniform exponentially small error. Evaluating the resulting Gaussian integral gives the desired result. $\square$

For our purposes, we will need a version of this valid in the neighborhood of a zero of F. Define polynomials $h_k(x)$ for integers $k \geq 0$ via the generating function

$$\sum_{k \geq 0} h_k(x) \frac{t^k}{k!} = e^{tx - t^2/2};$$

(2.37)

in particular, $h_k(x)$ is a monic polynomial of degree k, and

$$h_k(x) = \sum_{0 \leq j \leq [k/2]} (-1)^j \frac{k!}{2^j j!} \frac{x^{k-2j}}{(k-2j)!}$$

(2.38)

$$= \sum_{0 \leq j \leq k} \binom{k}{j} x^{k-j} h_j(0).$$

(2.39)

6

(Thus $h_k(x)$ are just rescaled Hermite polynomials.) In terms of $h_j(0)$, the above estimate becomes (replacing k by $k/2$):

$$\sqrt{2\pi r S'(r)n} r^{S(r)n} G(r)^{-n} [t^{S(r)n}] F(t) G(t)^n =$$
$$\sum_{0 \leq j \leq k} \frac{(rS'(r)n)^{-j/2} i^{-j} h_j(0)}{j!} \left(\frac{d^j}{dx^j} \gamma_x(r,x) F(re^{i\gamma(r,x)}) \right)_{x=0} + O(n^{-(k+1)/2}). \quad (2.40)$$

Corollary 2.5. *With hypotheses as in Lemma 2.4, suppose F has a zero of order k at the point $r_0 \in [r_1, r_2]$. Then we have the uniform asymptotic estimate*

$$\frac{[t^{S(r)n}]F(t)G(t)^n}{[t^{S(r)n}]G(t)^n} = \frac{F^{(k)}(r_0)}{k!} \frac{h_k\big((r - r_0)\sqrt{S'(r_0)n/r_0}\big)}{(S'(r_0)n/r_0)^{k/2}} + O(\max(|r - r_0|, n^{-1/2})^{k+1}), \quad (2.41)$$

valid for $r_1 \leq r \leq r_2$.

Proof. Since the main term of the estimate has order $O(|r - r_0|^k)$, we can tolerate a multiplicative error of order $1 + O(n^{-1/2})$. In particular, we may replace $[t^{S(r)n}]G(t)^n$ by its first-order estimate. We thus need to estimate (2.40).

Now,

$$\gamma_x(r,x) F(re^{i\gamma(r,x)}) = \sum_{0 \leq l} ((r\frac{d}{dr})^l F)(r) \gamma_x(r,x) \gamma(r,x)^l \frac{i^l}{l!} \quad (2.42)$$

$$= \sum_{0 \leq l} ((r\frac{d}{dr})^l F)(r) \frac{d}{dx} \gamma(r,x)^{l+1} \frac{i^l}{(l+1)!} \quad (2.43)$$

$$= \sum_{0 \leq j} \frac{x^j}{j!} \sum_{0 \leq l \leq j} \frac{i^l}{(l+1)!} ((r\frac{d}{dr})^l F)(r) \left((\frac{d}{dx})^{j+1} h(r,x)^{l+1} \right)_{x=0}. \quad (2.44)$$

Thus we obtain

$$\sum_{0 \leq j \leq k} \frac{(rS'(r)n)^{-j/2} h_j(0) i^{-j}}{j!} \sum_{0 \leq l \leq j} \frac{i^l}{(l+1)!} ((r\frac{d}{dr})^l F)(r) \left((\frac{d}{dx})^{j+1} \gamma(r,x)^{l+1} \right)_{x=0}. \quad (2.45)$$

Now, for $0 \leq l \leq k$,

$$(r\frac{d}{dr})^l F(r) = O((r - r_0)^{k-l}), \quad (2.46)$$

and for $l \leq j$, we have:

$$\left((\frac{d}{dx})^{j+1} \gamma(r,x)^{l+1} \right)_{x=0} = O(1). \quad (2.47)$$

In particular, the j, l term gives a contribution of order $O(|r - r_0|^{k-l} n^{-j/2})$. For fixed l, the contributions get smaller as j increases. We thus find that the terms with $l < j \leq k$ are dominated by the terms with $j = l + 1$, of order

$$O(|r - r_0|^{k-l} n^{-(l+1)/2}) = O(\max(|r - r_0|, n^{-1/2})^{k+1}). \quad (2.48)$$

7

It remains to consider the terms with $j = l$, that is,

$$\sum_{0 \leq l \leq k} \frac{(rS'(r)n)^{-l/2} h_l(0)}{l!} ((r\frac{d}{dr})^l F)(r). \tag{2.49}$$

If we replace $r\frac{d}{dr}$ by $r_0\frac{d}{dr}$, $F(r)$ by $F^{(k)}(r_0)(r - r_0)^k/k!$ and $rS'(r)$ by $r_0 S'(r_0)$, the resulting error is again $O(\max(|r - r_0|, n^{-1/2})^{k+1})$. We thus obtain

$$\frac{F^{(k)}(r_0)}{k!} \sum_{0 \leq l \leq k} \sqrt{S'(r_0)n/r_0}^{-l} \frac{h_l(0)}{(S'(r_0)n/r_0)^{l/2}} \binom{k}{l} (r - r_0)^{k-l} = \frac{F^{(k)}(r_0)}{k!} \frac{h_k(\sqrt{S'(r_0)n/r_0}(r - r_0))}{(S'(r_0)n/r_0)^{k/2}} \tag{2.50}$$

as required.
$\square$

We conclude with one more analytical lemma, used in Section 5 below.

Lemma 2.6. *Let $F(t)$ and $G(t)$ be real power series convergent on the circle $|t| < r$. Suppose $G \succeq 0$, with $G(0)$, $G'(0)$ both positive. Let I be a compact subset of $[0, r)$ on which F is positive. Then for all sufficiently large l, the holomorphic functions*

$$F(a)G(a)^l + F(-a)G(-a)^l \quad and \quad \frac{F(a)G(a)^l - F(-a)G(-a)^l}{a} \tag{2.51}$$

are positive on I.

Proof. We first note that if I does not contain 0, then $|G(-a)/G(a)|$ is bounded below 1 on I, while $|F(-a)/F(a)|$ is bounded; the result follows immediately. If I is the single point $\{0\}$, then $F(0) > 0$ by assumption, so $F(x) > 0$ for sufficiently small positive x; we may thus enlarge I while maintaining the hypotheses. We may thus take I of the form $[0, \epsilon]$ with $\epsilon > 0$; moreover, if the theorem is true for $[0, \epsilon']$ with $0 < \epsilon' < \epsilon$, it is true for $[0, \epsilon]$.

Since $F(0)$ and $G(0)$ are both positive, we may choose ϵ so that $F(a)$ and $G(a)$ are positive on $[-\epsilon, \epsilon]$. In particular, the first function is thus positive on $[0, \epsilon]$ for all l; it remains to consider the second function.

Now, clearly $(F(a) - F(-a))/a$ is analytic on $[-\epsilon, \epsilon]$, while

$$\frac{\log G(a) - \log G(-a)}{a} \tag{2.52}$$

is real analytic and positive on $[-\epsilon, \epsilon]$. In particular, there exist positive constants C_1 and C_2 such that

$$|F(a) - F(-a)| \leq C_1 a \tag{2.53}$$

$$C_2 a \leq \log G(a) - \log G(-a). \tag{2.54}$$

We thus find:

$$\frac{F(a)G(a)^l - F(-a)G(-a)^l}{a} = G(-a)^l \frac{F(a) - F(-a)}{a} + F(a)G(-a)^l \frac{e^{l(\log G(a) - \log G(-a))} - 1}{a} \tag{2.55}$$

$$\geq G(-a)^l \left(\frac{F(a) - F(-a)}{a} + F(a) \frac{\log G(a) - \log G(-a)}{a} \right) \tag{2.56}$$

$$\geq G(-a)^l (F(a)C_2 l - C_1), \tag{2.57}$$

which is clearly positive for sufficiently large l.
$\square$

8

3   The main theorem

Given a power series (or left-finite Laurent series) p, we define the valuation $\nu(p)$ of p to be the exponent of the first nonzero term in p.

The general scenario we consider is as follows. We are given power series $f(t)$, $g(t)$, and $h(t)$, and asked to prove a statement of the following form. If

$$A(t) = h(t) \sum_{0 \leq i \leq m} c_i f(t)^{m-i} g(t)^i \tag{3.1}$$

is such that $A \succeq 0$, then $\nu(A - 1) \lesssim \delta m$ as $m \to \infty$. (By this, we mean that if ν_m is the maximum possible value for given m, then $\limsup_{m \to \infty} \nu_m / m \leq \delta$.)

We make the normalizing assumptions $f(0) = 1$, $h(0) = 1$, $g(0) = 0$, $g'(0) = 1$. (We could also assume $f'(0) = 0$, but this is somewhat unnatural in the cases of interest.)

In this context, we recall the following variant of the Bürmann-Lagrange theorem:

Lemma 3.1. *Let $\phi(t)$ and $\psi(t)$ be formal power series, where $\psi(0) = 0$, $\psi'(0) \neq 0$. Then*

$$\phi(t) = \sum_{0 \leq i} \kappa_i \psi(t)^i, \tag{3.2}$$

where

$$\kappa_i = [t^0] \phi(t) \frac{t \psi'(t)}{\psi(t)} \psi(t)^{-i}. \tag{3.3}$$

The advantage of this formulation for our purposes is that the dependence on j below is encoded in a single power series.

Corollary 3.2. *Let the coefficients a_j and c_i be related by the formal power series identity*

$$\sum_{j \geq 0} a_j t^j = h(t) \sum_{i \geq 0} c_i f(t)^{m-i} g(t)^i, \tag{3.4}$$

with f, g, h as above. Then

$$c_i = \sum_j \alpha_{ij} a_j, \tag{3.5}$$

where

$$\alpha_{ij} = [t^0] t^j h(t)^{-1} f(t)^{i-m} g(t)^{-i} \left[\frac{t g'(t)}{g(t)} - \frac{t f'(t)}{f(t)} \right]. \tag{3.6}$$

Proof. We write

$$t^j = h(t) \sum_{i \geq 0} \alpha_{ij} f(t)^{m-i} g(t)^i, \tag{3.7}$$

and thus

$$h(t)^{-1} f(t)^{-m} t^j = \sum_{i \geq 0} \alpha_{ij} \left(\frac{g(t)}{f(t)} \right)^i; \tag{3.8}$$

the formula follows immediately from the lemma. $\qquad\qquad\square$

In particular,

Corollary 3.3. *Let f, g, h be as above, and suppose*

$$\sum_j a_j t^j = h(t) \sum_{0 \le i \le m} c_i f(t)^{m-i} g(t)^i. \tag{3.9}$$

Then for all $i > m$,

$$\sum_j \alpha_{ij} a_j = 0. \tag{3.10}$$

We will thus need an asymptotic analysis of the coefficients α_{ij}. In fact, until Section 6 we will need only the cases $i = m + 1$ and $i = m + 2$.

To make the asymptotic analysis tractable, we need some additional assumptions (summarized in the statement of Theorem 3.6 below). First, we assume $f \succeq 0$, $f \not\equiv 1$; in all of our applications, f is derived from a weight enumerator or theta series, so this condition is automatic. Our second condition, that $1/g \succeq 0$, is less automatic, but is easily verified in all cases of interest.

Define a function $Lg(t) = tg'(t)/g(t)$. By Lemma 2.2 applied to the Laurent series $1/g$, we find $Lg'(t) < 0$ for positive t within the radius of convergence of $1/g$. Thus if the equation $Lg(t) = 0$ has a positive real root, it must be unique. We assume the root exists, and denote it by t_0. Note that if $1/g$ has radius of convergence r, and $\lim_{t \to r^-} g(t) = 0$, then $1/g(t)$ is eventually increasing, and thus $Lg(t)$ is eventually negative; since $Lg(0) = 1 > 0$, this implies that $Lg(t) = 0$ has a positive real root.

We finally assume that t_0 is within the open disc of convergence of $f(t)$, $f(t)/h(t)$, and $f'(t)/h(t)$, and that $1/h(t) > 0$ on $[0, t_0]$.

Lemma 3.4. *Let f and g satisfy the above conditions. Then $f(t)/g(t)$ has a unique local minimum on $(0, t_0)$.*

Proof. Since $f/g \succeq 0$, we conclude that $f(e^s)/g(e^s)$ is strictly convex on $(-\infty, \log t_0)$. Now, $\lim_{t \to 0} f(t)/g(t) = +\infty$, and thus $f(e^s)/g(e^s)$ is decreasing in a neighborhood of $s = -\infty$. It thus remains only to show that $f(t)/g(t)$ is increasing near t_0.

We compute:

$$t \frac{d}{dt} \frac{f(t)}{g(t)} = g(t)^{-1}(f'(t) - Lg(t)f(t)). \tag{3.11}$$

At t_0, this becomes $f'(t)/g(t) > 0$. $\qquad\square$

Denote this local minimum by t_1.

Lemma 3.5. *Let f, g satisfy the above assumptions. Then there exists a unique point t_0' in $(0, t_0)$ such that*

$$\frac{f(t_0')}{g(t_0')} = \frac{f(t_0)}{g(t_0)}; \tag{3.12}$$

moreover, $t_0' < t_1$.

Proof. Uniqueness follows from strict convexity, so it suffices to show existence. But $f(t)/g(t)$ is continuous and decreasing on $(0, t_1]$, and converges to ∞ at 0, so attains every value greater than $f(t_1)/g(t_1)$, in particular $f(t_0)/g(t_0)$. $\qquad\square$

The basic idea behind the proof of Theorem 3.6 below is that, to first order, the relation corresponding to

$$c_{m+2} - \frac{f(t_0)}{g(t_0)} c_{m+1} \tag{3.13}$$

is 0 at $j = 0$ and is positive for $j > Lg(t_0')m$. Moreover, if we perturb the relation by subtracting a small multiple of c_{m+1}, the relation becomes positive at $j = 0$, at the cost of slightly reducing the range of positivity. I.e., we can use Lemma 2.3 to obtain a contradiction for all relaxations of the desired bound when m is sufficiently large.

Theorem 3.6. *Let f, g, and h be convergent real power series satisfying the following hypotheses:*

(i). $f, h = 1 + O(t)$, $g = t + O(t^2)$.

(ii). $f, 1/g \succeq 0$.

(iii). $Lg(t) := tg'(t)/g(t)$ has a positive real zero; let the smallest such zero be denoted t_0.

(iv). f, $1/g$, f/h, and f'/h have radius of convergence $> t_0$.

(v). $1/h$ is positive on $[0, t_0]$.

For each integer $m \geq 0$, let d_m be the maximum of $\nu(A - 1)$ where A ranges over power series $\succeq 0$ of the form

$$A(t) = h(t) \sum_{0 \leq i \leq m} c_i f(t)^{m-i} g(t)^i. \tag{3.14}$$

Then $\limsup_{m \to \infty} d_m/m \leq Lg(t_0')$, where $0 < t_0' < t_0$ is such that $f(t_0')/g(t_0') = f(t_0)/g(t_0)$.

Proof. Choose $0 < t_2 < t_0'$; we will show that for all sufficiently large m, $d_m/m \leq Lg(t_2)$. As this will hold for all choices of t_2, the theorem will follow from the continuity of Lg. We also choose $0 < t_3 < t_2$.

We consider the linear combination $c_{m+2} - f(t_3)/g(t_3)c_{m+1}$, as a vanishing linear combination of the coefficients of $A(t)$. In particular, if we let $\alpha_j(t_3)$ denote the coefficient of $[t^j]A(t)$ in this linear combination, it will suffice to show that for all sufficiently large m, $\alpha_j(t_3) > 0$ for $j = 0$ and $j \geq Lg(t_2)m$. Indeed, if a choice of $A(t)$ existed with $d_m \geq Lg(t_2)m$, this would give a positive linear combination of nonnegative quantities (at least one of which is positive), equal to 0, a contradiction.

We compute:

$$\alpha_j(t_3) = \alpha_{(m+2)j} - \frac{f(t_3)}{g(t_3)} \alpha_{(m+1)j} \tag{3.15}$$

$$= [t^0] t^j \left(\frac{f(t)}{g(t)h(t)} \right) \left(\frac{f(t)}{g(t)} - \frac{f(t_3)}{g(t_3)} \right) \left(\frac{tg'(t)}{g(t)} - \frac{tf'(t)}{f(t)} \right) g(t)^{-m} \tag{3.16}$$

$$= -[t^{m+2-j}] t^3 \left(\frac{1}{h(t)} \right) \left(\frac{f(t)}{g(t)} - \frac{f(t_3)}{g(t_3)} \right) \frac{d}{dt} \left(\frac{f(t)}{g(t)} \right) \tilde{g}(t)^{-m}, \tag{3.17}$$

11

where $\tilde{g}(t) := t^{-1}g(t)$. We thus need to show that for all sufficiently large m,

$$[t^k]F(t)G(t)^m > 0 \tag{3.18}$$

for $k = m + 2$ and $0 \le k \le (1 - Lg(t_2))m$, where

$$G(t) = \tilde{g}(t)^{-1}, \tag{3.19}$$

$$F(t) = t^3 h(t)^{-1}\left(\frac{f(t_3)}{g(t_3)} - \frac{f(t)}{g(t)}\right)\frac{d}{dt}\left(\frac{f(t)}{g(t)}\right). \tag{3.20}$$

We note the following properties:

(i). $F(t)$ and $G(t)$ are power series with radius of convergence $> t_0$.

(ii). $G(t) \succeq 0$.

(iii). $F(t_0) > 0$. Indeed, the first two factors are clearly positive, while the second factor is positive since

$$\frac{f(t_0)}{g(t_0)} = \frac{f(t_0')}{g(t_0')} < \frac{f(t_3)}{g(t_3)}. \tag{3.21}$$

Similarly, the third factor is positive, since $t_0 > t_1$.

(iv). $F(t)$ is positive on $[0, t_3)$. This time, the second and third factors are negative; we note the limit $F(0) = 1$.

In other words, the hypotheses of Lemma 2.3 apply, taking $I = [0, t_2] \cup [t_0, t_0 + \epsilon]$ for appropriate $\epsilon > 0$. It follows that for all sufficiently large m,

$$[t^j]F(t)G(t)^m > 0 \tag{3.22}$$

when $j/m \in [0, 1 - Lg(t_2)] \cup [1, 1 - Lg(t_0 + \epsilon)]$. For sufficiently large m, $(m + 2)/m \in [1, 1 - Lg(t_0 + \epsilon)]$, so we are done. $\qquad\square$

Example. Let $A(x, y)$ be the weight enumerator of a doubly-even binary self-dual code of length n. Then by Gleason's theorem, we have:

$$A(x, y) = \sum_{0 \le i \le [n/24]} c_i(x^8 + 14x^4 y^4 + y^8)^{n/8 - 3i}(x^4 y^4(x^4 - y^4)^4)^i. \tag{3.23}$$

Defining a power series $A(t)$ by $A(t) = A(1, t^{1/4})$, we obtain:

$$A(t) = \sum_{0 \le i \le [n/24]} c_i(1 + 14t + t^2)^{n/8 - 3i}(t(1 - t)^4)^i \tag{3.24}$$

$$= (1 + 14t + t^2)^{n/8 - 3[n/24]} \sum_{0 \le i \le [n/24]} c_i((1 + 14t + t^2)^3)^{[n/24] - i}(t(1 - t)^4)^i. \tag{3.25}$$

We will apply the main theorem, with

$$f(t) = (1 + 14t + t^2)^3 \tag{3.26}$$

$$g(t) = t(1 - t)^4 \tag{3.27}$$

$$h(t) = (1 + 14t + t^2)^{n/8 - 3[n/24]}. \tag{3.28}$$

12

We clearly have $f, 1/g, h \succeq 0$, and each of f, $1/g$, f/h, f'/h has radius of convergence at least 1; indeed, except for $1/g$, these are polynomials. Since $\lim_{t \to 1} g(t) = 0$, the hypotheses of Theorem 3.6 are satisfied.

We easily compute $t_0 = 1/5$; we then find that t_0' is the unique solution in $(0, 1/5)$ of the quartic equation

$$t^4 - 644t^3 + 6t^2 - 644t + 1. \tag{3.29}$$

We thus obtain the bound

$$\limsup_{m \to \infty} \frac{d_m}{m} \leq \frac{1 - 5t_0'}{1 - t_0'}, \tag{3.30}$$

or, since $\nu(A(t) - 1) = d(C)/4$ and $m = [n/24]$,

$$\limsup_{n \to \infty} \frac{d(C)}{n(C)} \leq \frac{1 - 5t_0'}{6(1 - t_0')}. \tag{3.31}$$

In fact (as we will explain below), t_0' has the simple closed form

$$t_0' = \left(\frac{1 - 5^{-1/4}}{1 + 5^{-1/4}} \right)^4 ; \tag{3.32}$$

when substituted in, this simplifies (again explained below) to give

$$\limsup_{n \to \infty} d_n/n \leq \frac{1}{2}(1 - 5^{-1/4}). \tag{3.33}$$

4 Applications I

We generalize the previous example as follows (compare the Gleason-Pierce theorem [20]):

Theorem 4.1. *Let q and c be chosen with $q > 1$, such that either $c = 1$ or $(q, c) \in \{(2, 2), (2, 4), (3, 3), (4, 2)\}$. Let C_i be a sequence of formally self-dual codes over an alphabet of size q with all Hamming weights divisible by c; suppose furthermore that as $i \to \infty$, $n(C_i) \to \infty$. Then*

$$\limsup_{i \to \infty} \frac{d(C_i)}{n(C_i)} \leq \frac{q - 1}{q}(1 - (c + 1)^{-1/c}). \tag{4.1}$$

Proof. Given such a code C, of length n, let $A_C(x, y)$ be its weight enumerator, and define a power series $A(t) = A_C(1, t^{-1/c})$. Then from the various Gleason theorems [18, Section 7], we conclude

$$c = 1 : A(t) = (1 + (\sqrt{q} - 1)t)^{n \bmod 2} \sum_{0 \leq i \leq [n/2]} c_i((1 + (\sqrt{q} - 1)t)^2)^{[n/2] - i}(t(1 - t))^i \tag{4.2}$$

$$(q, c) = (2, 2) : A(t) = (1 + t)^{(n/2) \bmod 4} \sum_{0 \leq i \leq [n/8]} c_i((1 + t)^4)^{[n/8] - i}(t(1 - t)^2)^i \tag{4.3}$$

$$(q, c) = (2, 4) : A(t) = (1 + 14t + t^2)^{(n/8) \bmod 3} \sum_{0 \leq i \leq [n/24]} c_i((1 + 14t + t^2)^3)^{[n/24] - i}(t(1 - t)^4)^i \tag{4.4}$$

$$(q, c) = (3, 3) : A(t) = (1 + 8t)^{(n/4) \bmod 3} \sum_{0 \leq i \leq [n/12]} c_i((1 + 8t)^3)^{[n/12] - i}(t(1 - t)^3)^i \tag{4.5}$$

$$(q, c) = (4, 2) : A(t) = (1 + 3t)^{[n/2] \bmod 3} \sum_{0 \leq i \leq [n/6]} c_i((1 + 3t)^3)^{[n/6] - i}(t(1 - t)^2)^i, \tag{4.6}$$

13

for appropriate coefficients c_i. In particular, we are in the scenario of Theorem 3.6, with $g(t) = t(1-t)^c$. In each case, f, f/h and f'/h are all clearly polynomials; since $1/g \succeq 0$, has radius of convergence 1, and $g(1) = 0$, the hypotheses of the theorem are satisfied; it remains to compute $Lg(t'_0)$.

Since

$$Lg(t) = \frac{1 - (1+c)t}{1-t}, \tag{4.7}$$

we find $t_0 = 1/(1+c)$. To compute t'_0 from t_0, we proceed as follows.

Define new series $F(t) = f(t^c)$ and $G(t) = g(t^c)$. From the MacWilliams identity and the fact that f and g are linear combinations of power series coming from weight enumerators, we find that there exists an integer n_0 such that:

$$F\left(\frac{1-t}{1+(q-1)t}\right) = q^{n_0/2}(1+(q-1)t)^{-n_0}F(t) \tag{4.8}$$

$$G\left(\frac{1-t}{1+(q-1)t}\right) = q^{n_0/2}(1+(q-1)t)^{-n_0}G(t). \tag{4.9}$$

Dividing these equations, we find

$$\frac{F}{G}\left(\frac{1-t}{1+(q-1)t}\right) = \frac{F}{G}(t). \tag{4.10}$$

In terms of f and g, this becomes:

$$\frac{f}{g}\left(\left(\frac{1-t^{1/c}}{1+(q-1)t^{1/c}}\right)^c\right) = \frac{f}{g}(t). \tag{4.11}$$

We thus conclude that

$$t'_0 = \left(\frac{1 - (c+1)^{-1/c}}{1+(q-1)(c+1)^{-1/c}}\right)^c, \tag{4.12}$$

since we readily verify $0 < t'_0 < t_0$.

Similarly, to compute $Lg(t'_0)$, we differentiate the functional equation for G at $t_0^{1/c}$, obtaining:

$$Lg(t'_0) = \frac{(q-1)n_0}{cq}(1-t_0^{1/c}) + Lg(t_0)\left(\frac{(q-1)t_0^{1/c} - (q-2) - t_0^{-1/c}}{q}\right) = \frac{(q-1)n_0}{cq}(1-t_0^{1/c}), \tag{4.13}$$

since by definition $Lg(t_0) = 0$. Since $m = [n/n_0]$ and $\nu(A(t) - 1) = d(C)/c$, we mutiply this by c/n_0 to obtain the desired bound. $\square$

Remark. In particular:

  (i). For doubly-even self-dual binary codes, $d/n \lesssim (1 - 5^{-1/4})/2 = .1656298476$.

  (ii). For self-dual ternary codes, $d/n \lesssim (2 - 2^{1/3})/3 = .2466929834$.

  (iii). For even self-dual additive codes over $GF(4)$, $d/n \lesssim (3 - 3^{1/2})/4 = .3169872982$.

  (iv). For singly-even, formally self-dual binary codes, $d/n \lesssim (1 - 3^{-1/2})/2 = .2113248655$.

14

(v). For formally self-dual codes over $GF(q)$, $d/n \lesssim 1/2 - 1/2q$.

Strictly speaking only the case $(q,c) = (3,3)$ is new; the case $(q,c) = (2,4)$ was shown (via a rather different proof) in [7], while in the remaining cases, the bound obtained is worse than the JPL [11] or Aaltonen [1], [2] bound, as appropriate. But for singly-even self-dual binary codes, see Theorem 5.1 below.

For even modular lattices (see [12], [13], [19]; note that a unimodular lattice is 1-modular), we proceed similarly. We recall Dedekind's η function

$$\eta(z) = e^{\pi i z/12} \prod_i (1 - e^{2\pi i m z}) \tag{4.14}$$

and the Eisenstein series

$$E_2(z) = \frac{1}{2\pi i} \frac{d}{dz} \log \eta(z) \tag{4.15}$$

$$= \frac{1}{24} - \sum_{1 \le m} (\sum_{k|m} k) e^{2\pi i m z}. \tag{4.16}$$

Theorem 4.2. *Let N be one of the integers $\{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$, and define*

$$E_2^{(N)}(z) = \sum_{m|N} m E_2(mz). \tag{4.17}$$

Then for any sequence Λ_i of even, strongly N-modular lattices of dimension tending to ∞,

$$\limsup_{i \to \infty} \frac{\mu(\Lambda_i)}{\dim(\Lambda_i)} \le \frac{N z_0}{2\pi i}, \tag{4.18}$$

where z_0 is the unique zero of $E_2^{(N)}$ on the positive imaginary axis.

Proof. Let Λ be an even, strongly N-modular lattice, with theta series Θ_Λ. Then ([12],[13]) $\Theta_\Lambda(e^{\pi i z})$ can be written as a weighted-homogeneous polynomial in $\Theta_{\Lambda_0}(e^{\pi i z})$ and $g(e^{2\pi i z}) = (\prod_{m|N} \eta(mz))^{24/(\sum_{m|N} m)}$, where Λ_0 is the lowest-dimensional even N-modular lattice.

Clearly $\Theta_{\Lambda_0}(t^{1/2}) \succeq 0$; using the product formula for η, we also conclude that $1/g(t) \succeq 0$. Thus Theorem 3.6 applies, and it remains only to compute $Lg(t_0')$.

We first compute, with $t = e^{2\pi i z}$,

$$Lg(z) = \frac{1}{2\pi i} \frac{d}{dz} \log \prod_{m|N} \eta(mz)^{24/(\sum_{m|N} m)} \tag{4.19}$$

$$= \frac{24}{\sum_{m|N} m} E_2^{(m)}(z), \tag{4.20}$$

and thus $t_0 = e^{2\pi i z_0}$.

We have the transformation laws:

$$f(-1/Nz) = N^{n_0/4}(z/i)^{n_0/2} f(z) \tag{4.21}$$

$$g(-1/Nz) = N^{n_0/4}(z/i)^{n_0/2} g(z), \tag{4.22}$$

15

where

$$n_0 = \frac{24\delta(N)}{\sum_{m|N} m}. \tag{4.23}$$

We thus conclude that $t'_0 = e^{-2\pi i/Nz_0}$, and that

$$Lg(t'_0) = \frac{z_0 N n_0}{4\pi i} + N z_0^2 Lg(t_0) = \frac{z_0 N n_0}{4\pi i}. \tag{4.24}$$

Multiplying by 2 (since the lattices are even) and dividing by n_0 (since $m = [n/n_0]$) gives the required bound. $\square$

Remark. Numerically, we have:

$$N = 1 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .0833210664 \qquad N = 2 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .1246710056$$

$$N = 3 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .1643714543 \qquad N = 5 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .2351529896$$

$$N = 6 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .2414115212 \qquad N = 7 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .2957105217$$

$$N = 11 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .3973198712 \qquad N = 14 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .4266498017$$

$$N = 15 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .3206725342 \qquad N = 23 : \frac{\mu(\Lambda)}{\dim(\Lambda)} \lesssim .6262824896$$

Again, aside from $N = 1$, $N = 2$, $N = 3$, the obtained bound is worse than that implied by the Kabatiansky-Levenshtein bound on sphere packings [6].

We finally consider self-dual codes over $\mathbb{Z}_4$. As in [14], bounding the Hamming or Lee distance reduces to a consideration of the dual distance of doubly-even binary codes. At length a multiple of 8, the bound on self-dual doubly-even codes applies; for other lengths, we shorten the code up to 7 times, without affecting the asymptotic bound. We thus obtain:

Theorem 4.3. *Let C_i be a sequence of self-dual codes over $\mathbb{Z}_4$, with length tending to ∞. Then*

$$\limsup_{i \to \infty} \frac{d_H(C_i)}{n(C_i)} \leq \frac{1 - 5^{-1/4}}{2} \tag{4.25}$$

$$\limsup_{i \to \infty} \frac{d_L(C_i)}{n(C_i)} \leq 1 - 5^{-1/4}, \tag{4.26}$$

where $d_H(C)$ and $d_L(C)$ are the minimum Hamming and Lee weights of C, respectively.

For the Euclidean distance, the situation is more complicated. We use the following lemma:

Lemma 4.4. *Let C be a Type II self-dual code over $\mathbb{Z}_4$ (all Euclidean norms divisible by 8), and let $A(x, y, z)$ be its symmetrized weight enumerator. Define a power series*

$$A(t) := A(1, 2^{-1/4} t^{1/8} (1 + t)^{1/4}, t^{1/2}). \tag{4.27}$$

16

Then $A \succeq 0$, and

$$\nu(A(t) - 1) = d_E(C)/8. \tag{4.28}$$

Moreover, for appropriate coefficients c_i,

$$A(t) = \sum_{0 \le i \le [n/24]} c_i(1 + 60t + 134t^2 + 60t^3 + t^4)^{(n/8)-3i}(t(1-t)^6(1-t^2)^2)^i. \tag{4.29}$$

Proof. Consider a monomial $x^a y^b z^c$ of $A(x, y, z)$; note that $b + 4c$ must be a multiple of 8, and in particular b is a multiple nof 4. Under the specified substitution, this yields

$$2^{-b/4}(1+t)^{b/4}t^{(b+4c)/8}, \tag{4.30}$$

a polynomial with nonnegative coefficients and with valuation $(b + 4c)/8$; the first two claims are immediate.

Now, the Gleason theorem for Type II codes over $\mathbb{Z}_4$ states that $A(x, y, z)$ is a (weighted homogeneous) polynomial in

$$\theta_8 = \frac{(x+z)^8 + (x-z)^8}{2} + 128y^8 \tag{4.31}$$

$$\theta_{16} = (x^2z^2(x^2+z^2)^2 - 4y^8)((x^4 + 6x^2z^2 + z^4)^2 - 64y^8) \tag{4.32}$$

$$\theta_{24} = y^8(x^2 - z^2)^8 \tag{4.33}$$

$$h_8 = (xz(x^2+z^2) - 2y^4)^2. \tag{4.34}$$

Under the substituion, we have:

$$\theta_8 \mapsto 1 + 60t + 134t^2 + 60t^3 + t^4 \tag{4.35}$$

$$\theta_{16} \mapsto 0 \tag{4.36}$$

$$\theta_{24} \mapsto \frac{1}{4}t(1-t)^6(1-t^2)^2 \tag{4.37}$$

$$h_8 \mapsto 0 \tag{4.38}$$

The remaining claim follows. $\qquad\square$

Remark. The above substitution is inspired by the proofs used in [4] and [19], which involve lifting the code to a lattice and analyzing the resulting theta series. The resulting substitution takes the polynomial

$$2y^4 - xz(x^2 + z^2) \tag{4.39}$$

to 0; solving gives the above substitution.

We apply Theorem 3.6 with $f(t) = (1 + 60t + 134t^2 + 60t^3 + t^4)^3$, $g(t) = t(1-t)^6(1-t^2)^2$, to obtain:

Theorem 4.5. *Let C_i be a sequence of Type II self-dual codes over $\mathbb{Z}_4$ with length tending to ∞. Then*

$$\limsup_{i \to \infty} \frac{d_E(C_i)}{n(c_i)} \le .3332625492 = 2 - 2x, \tag{4.40}$$

where x is the positive real root of the polynomial

$$11x^{16} + 2112x^{14} - 8525x^{12} + 15048x^{10} - 15218x^8 + 9552x^6 - 3718x^4 + 828x^2 - 81. \tag{4.41}$$

17

Remark 1. The field $\mathbb{Q}[x]$ is that generated by

$$2^{-1/4}t_0^{1/8}(1+t_0)^{1/4} \text{ and } t_0^{1/2}, \tag{4.42}$$

where $t_0 = \frac{2\sqrt{5}-3}{11}$.

Remark 2. The Type II hypothesis is removed in Theorem 5.3 below.

5   Applications II

We now consider applications to which Theorem 3.6 does not directly apply, but for which the same basic idea can be used.

We first extend the bound for doubly-even self-dual binary codes to general self-dual binary codes. The main idea is that, using Lemma 2.6, we can reduce positivity of coefficients of the form

$$[t^j]F_1(t)F_2(t)^l G(t^2)^m \tag{5.1}$$

to positivity of $F_1(t)$, for all sufficiently large l and all sufficiently large m; this because

$$[t^{2j}]F_1(t)F_2(t)^l G(t^2)^m = [t^j]\left(F_1(\sqrt{t})F_2(\sqrt{t})^l + F_1(-\sqrt{t})F_2(-\sqrt{t})^l\right)G(t)^m \tag{5.2}$$

$$[t^{2j+1}]F_1(t)F_2(t)^l G(t^2)^m = [t^j]\left(\frac{F_1(\sqrt{t})F_2(\sqrt{t})^l - F_1(-\sqrt{t})F_2(-\sqrt{t})^l}{\sqrt{t}}\right)G(t)^m. \tag{5.3}$$

Theorem 5.1. *Let C_i be a sequence of self-dual binary codes of length tending to ∞. Then*

$$\limsup_{i\to\infty}\frac{d(C_i)}{n(C_i)} \le \frac{1-5^{-1/4}}{2}. \tag{5.4}$$

Proof. We recall that a self-dual binary code C has associated to it two enumerators: its weight enumerator $A(x,y)$ and its "shadow" enumerator $S(x,y)$ [5], [18].[1] For appropriate coefficients c_i, we have:

$$A(x,y) = (x^2+y^2)^{(n\bmod 8)/2}\sum_{0\le i\le [n/8]}c_i((x^2+y^2)^4)^{[n/8]-i}(x^2y^2(x^2-y^2)^2)^i \tag{5.5}$$

$$S(x,y) = (2xy)^{(n\bmod 8)/2}\sum_{0\le i\le [n/8]}c_i((2xy)^4)^{[n/8]-i}(-(x^4-y^4)^2/4)^i \tag{5.6}$$

Here c_i can be characterized (up to a multiplicative constant) as the unique linear combination of the first $i+1$ nontrivial coefficients of $A(x,y)$ that is also a linear combination of the first $[n/8]-i$ nontrivial coefficients of $S(x,y)$.

We define power series $A(t)$ and $S(t)$ by

$$A(t) = A(1,t^{1/2}) \tag{5.7}$$

$$= (1+t)^{(n\bmod 8)/2}\sum_{0\le i\le [n/8]}c_i((1+t)^4)^{[n/8]-i}(t(1-t)^2)^i \tag{5.8}$$

$$S(t) = t^{-(n\bmod 8)/8}S(1,t^{1/4}) \tag{5.9}$$

$$= 2^{(n\bmod 8)/2}\sum_{0\le i\le [n/8]}c_i(16t)^{[n/8]-i}(-(1-t)^2/4)^i. \tag{5.10}$$

---

[1]Note that this includes the doubly-even case, for which $S(x,y) = A(x,y)$.

If we let α_{ij} denote the coefficient of $[t^j]A(t)$ in c_i, and let β_{ij} denote the coefficient of $[t^j]S(t)$ in c_i, Bürmann-Lagrange tells us:

$$\alpha_{ij} = [t^{i-j}](1 - 6t + t^2)(1+t)^{4i-n/2-1}(1-t)^{-2i-1} \tag{5.11}$$

$$= [t^{i-j}](1 - 6t + t^2)(1+t)^{6i-n/2}(1-t^2)^{-2i-1} \tag{5.12}$$

$$\beta_{ij} = (-1)^i 2^{6i-n/2}[t^{[n/8]-i-j}](1+t)(1-t)^{-2i-1}. \tag{5.13}$$

Set $t_0 = 5^{-1/2}$, $t_0' = \left(\frac{1-5^{-1/4}}{1+5^{-1/4}}\right)^2$, and let m be an even integer of the form $n/12 + l/6$. Now, consider the coefficient

$$c_{m+1} - \frac{(1+t_0)^4}{t_0(1-t_0)^2}c_m. \tag{5.14}$$

This is manifestly a negative linear combination of $[t^j]S(t)$ for $0 \le j \le [n/8] - m$ (so the same will be true for small perturbations). It thus suffices to consider the coefficients of $[t^j]S(t)$. By the remark above and Lemma 2.6, this reduces to showing that

$$(1 - 6t + t^2)\left(\frac{(1+t)^4}{t(1-t)^2} - \frac{(1+t_0)^4}{t_0(1-t_0)^2}\right) \tag{5.15}$$

is positive for $0 \le t < t_0'$, and can be perturbed to be positive at t_0 as well; this is clearly the case. $\square$

Similarly, the bound for even self-dual additive codes over $GF(4)$ extends to the general case; the resulting bound is still weaker than the Aaltonen bound, however. A similar remark applies to formally self-dual binary codes, with shadow defined by $S(x, y) = A(y, x)$; there the bound for singly-even f.s.d. binary codes extends. In that case, $m \sim n/4$, instead of the obvious analogue $n/3$; also we must apply Lemma 2.6 to the coefficients of S as well as to the coefficients of A.

For lattices, we have:

Theorem 5.2. *Let N be one of the integers $\{1, 2, 3, 5, 6, 7, 11, 14, 15, 23\}$, and define*

$$E_2^{(N)}(z) = \sum_{m|N} mE_2(mz). \tag{5.16}$$

Then for any sequence Λ_i of strongly N-modular lattices of dimension tending to ∞,

$$\limsup_{i\to\infty} \frac{\mu(\Lambda_i)}{\dim(\Lambda_i)} \le \frac{Nz_0}{2\pi i}, \tag{5.17}$$

where z_0 is the unique zero of $E_2^{(N)}$ on the positive imaginary axis.

Proof. As above; the case N odd is analogous to the self-dual binary code case, while the case N even is analogous to the formally self-dual binary code case. The only respect in which the proof is not straightforward (using the formulae of [19]) is in dealing with the "other" genera (not covered by Theorem 2 of [19]). In each case, direct summing by a suitable N-modular lattice places us into the "good" genera, and we can proceed from there; the only effect is to multiply the power series in question by a theta series, which clearly has no effect on positivity. $\square$

Our last shadow application is to codes over $\mathbb{Z}_4$:

Theorem 5.3. *Let C_i be a sequence of self-dual codes over $\mathbb{Z}_4$ with length tending to ∞. Then*

$$\limsup_{i \to \infty} \frac{d_E(C_i)}{n(c_i)} \leq .3332625492 = 2 - 2x, \tag{5.18}$$

where x is the positive real root of the polynomial

$$11x^{16} + 2112x^{14} - 8525x^{12} + 15048x^{10} - 15218x^8 + 9552x^6 - 3718x^4 + 828x^2 - 81. \tag{5.19}$$

Proof. We define

$$A(t) = A(1, 2^{-1/4}t^{1/4}(1+t^2)^{1/4}, t) \tag{5.20}$$

$$S(t) = t^{-(n \bmod 8)/8}(1+t)^{-(n \bmod 4)/4}S(1, 2^{-1/4}t^{1/8}(1+t)^{1/4}, t^{1/2}), \tag{5.21}$$

and observe that A and S are polynomials with nonnegative coefficients. Since

$$A(t) = \sum_{0 \leq i \leq [n/8]} c_i((1+t)^8)^{n/8-i}(t(1+t^2)(1-t)^4)^i \tag{5.22}$$

$$S(t) = (1+t)^{[n/4] \bmod 2} \sum_{0 \leq i \leq [n/8]} (-1)^i(64t(1+t)^2)^{[n/8]-i}((1-t)^4/8)^i, \tag{5.23}$$

we can proceed as in the case of self-dual binary codes. □

Our final application is to quantum codes. Formally, a q-ary quantum code corresponds to a self-orthogonal codes C over an alphabet of size q^2; the objective is to bound the minimum weight of the nonlinear code $C^\perp - C$. We recall the following (the nonbinary extension of [16, Theorem 6]):

Lemma 5.4. *Let Q be a q-ary quantum code of length n and dimension K. Then there exist polynomials $C(x,y)$ and $D(x,y)$, homogeneous of degree n, such that*

$$C(x,y) = C(\frac{x + (q^2-1)y}{q}, \frac{x-y}{q}) \tag{5.24}$$

$$D(x,y) = -D(\frac{x + (q^2-1)y}{q}, \frac{x-y}{q}), \tag{5.25}$$

$$C(1,0) = 1, \tag{5.26}$$

and satisfying

$$\nu(C(1,t) - D(1,t)) = d \tag{5.27}$$

$$C(1,t) \succeq \frac{K-1}{2K}(C(1,t) - D(1,t)) \tag{5.28}$$

$$C(1,t) - D(1,t) \succeq 0. \tag{5.29}$$

20

In particular, if C and D satisfy the constraints for a given value $K > 1$, they satisfy them for all smaller K, including for $K = 1$. Thus if we replace (5.28) by the condition

$$C(1, t) \succeq 0, \tag{5.30}$$

the resulting bound will apply to all quantum codes.

Theorem 5.5. *Let Q_i be a sequence of q-ary quantum codes of length tending to ∞. Then*

$$\limsup_{i \to \infty} \frac{d(Q_i)}{n(Q_i)} \leq \frac{1}{2} \left(1 - \frac{1}{q^2} \right). \tag{5.31}$$

Proof. We consider the case of odd length $n = 2m + 1$; the case of even length is analogous. Setting $C(t) := C(1, t)$, $D(t) = D(1, t)$, we observe that

$$C(t) = (1 + (q - 1)t) \sum_{0 \leq i \leq m} c_i((1 + (q - 1)t)^2)^{m-i}(t(1 - t))^i \tag{5.32}$$

$$D(t) = (1 - (q + 1)t) \sum_{0 \leq i \leq m} d_i((1 + (q - 1)t)^2)^{m-i}(t(1 - t))^i, \tag{5.33}$$

for suitable coefficients c_i and d_i. Let γ_{ij} be the coefficient of $[t^j]C(t)$ in c_i (extending as usual to $i > m$), and let δ_{ij} be the coefficient of $[t^j]D(t)$ in d_i. We find:

$$\gamma_{(m+1)j} = [t^{m+2-j}](1 - (q + 1)t)t(1 - t)(1 - t)^{-m-3} \tag{5.34}$$

$$\gamma_{(m+2)j} = [t^{m+2-j}](1 - (q + 1)t)(1 + (q - 1)t)^2(1 - t)^{-m-3} \tag{5.35}$$

$$\delta_{(m+1)j} = [t^{m+2-j}](1 + (q - 1)t)t(1 - t)(1 - t)^{-m-3} \tag{5.36}$$

$$\delta_{(m+2)j} = [t^{m+2-j}](1 + (q - 1)t)(1 + (q - 1)t)^2(1 - t)^{-m-3}. \tag{5.37}$$

If we instead expand c_i and d_i in terms of $[t^j]C(t)$ and $[t^j](C(t) - D(t))$, we obtain coefficients:

$$\big(\text{coeff. of } [t^j]C(t) \text{ in } c_i\big) = \gamma_{ij} \tag{5.38}$$

$$\big(\text{coeff. of } [t^j](C(t) - D(t)) \text{ in } c_i\big) = 0 \tag{5.39}$$

$$\big(\text{coeff. of } [t^j]C(t) \text{ in } d_i\big) = \delta_{ij} \tag{5.40}$$

$$\big(\text{coeff. of } [t^j](C(t) - D(t)) \text{ in } d_i\big) = -\delta_{ij} \tag{5.41}$$

We need a relation that is a nonnegative linear combination of the coefficients $[t^j]C(t)$, positive at $j = 0$, as well as a nonnegative linear combination of the coefficients $[t^j]C(t) - D(t)$ for j larger than the bound.

Now, consider the relation

$$(q + 1)(c_1 - (q + 1)^2 c_0) - (q - 1)(d_1 - (q + 1)^2 d_0). \tag{5.42}$$

On $[t^j]C(t) - D(t)$, this has coefficient:

$$(q - 1)[t^{m+2-j}](1 + (q - 1)t)(1 - 2t)(1 - (q^2 + 1)t)(1 - t)^{-m-3}, \tag{5.43}$$

21

which to first order is positive for $j/m > 1 - \frac{1}{q^2}$. Similarly, on $[t^j]C(t)$, this has coefficient:

$$2[t^{m+2-j}](1 - 2t)(1 - (q^2 + 1)t)^2(1 - t)^{-m-3} \tag{5.44}$$

which is positive for $0 \le j \le m + 2$ except in a neighborhood of $j = 0$ and $j = (1 - \frac{1}{q^2})m$. The construction of a positive perturbation is straightforward. $\square$

Similarly, taking the shadow constraints [17] into account, we obtain:

Theorem 5.6. *Let Q_i be a sequence of binary quantum codes of length tending to ∞. Then*

$$\limsup_{i \to \infty} \frac{d(Q_i)}{n(Q_i)} \le \frac{3 - \sqrt{3}}{4}. \tag{5.45}$$

Note that although as we have remarked, this is slightly worse than the Aaltonen bound, this is still a new result; in the quantum case, the Aaltonen bound is only known for a set of rates bounded above 0 [3].

6 Extensions

As we have remarked, many of our bounds are weaker than the appropriate "universal" bounds (JPL [11]; Aaltonen [1], [2]; Kabitiansky-Levenshtein [6]; see [8] for a survey) that hold even for non-self-dual codes of rate 1/2 and non-lattice packings of appropriate density. Since others of our bounds are quite a bit stronger than the corresponding universal bounds, this strongly suggests that in no case is either bound tight for self-dual codes. The question then becomes that of how to improve the above bounds.

We restrict our attention to the situation of Section 3; we will comment on the shadow and quantum cases at the end.

Thus, let f, g, h satisfy the hypotheses of Theorem 3.6. As the above bounds resulted from considering the two relations c_{m+1}, c_{m+2} in place of the single relation c_{m+1}, the obvious thing to try is a linear combination of c_{m+i} for $1 \le i \le l$. Somewhat surprisingly, this does not give rise to any improvement in terms of $\limsup d/m$. We can see this as follows. The coefficient of $[t^j]A(t)$ in such a linear combination will have the form

$$-[t^{m-j}]\left(\frac{1}{h(t)}\right)p(\frac{f(t)}{g(t)})t\frac{d}{dt}\left(\frac{f(t)}{g(t)}\right)\tilde{g}(t)^{-m}, \tag{6.1}$$

for some polynomial p. The point, then, is that since

$$\frac{d}{dt}\left(\frac{f(t)}{g(t)}\right) \tag{6.2}$$

has opposite signs at $t = t_0$ and at $t = t'_0$, while

$$\left(\frac{1}{h(t)}\right) \text{ and } p(\frac{f(t)}{g(t)}) \tag{6.3}$$

both have the same sign at the two points (the same value in the latter case), the corresponding coefficients will, to first order, also have opposite sign. In particular, we will never obtain a bound on d/m better than $Lg(t'_0)$. (This tends to explain why Krasikov and Litsyn obtained the same bound in the doubly-even binary case, despite a rather different argument, and the unlikelihood that the bound is optimal.)

On the other hand, we do obtain a slight lower-order improvement:

Theorem 6.1. *Let f, g, h, d_m, t_0, t_0' be as in the hypotheses of Theorem 3.6, and suppose further that*

$$\frac{t\left(\frac{d}{dt}\frac{f(t)}{g(t)}\right)^2}{-tLg'(t)} \tag{6.4}$$

is smaller at t_0 than at t_0'. Then

$$\limsup_{m\to\infty}\frac{d_m - Lg(t_0')m}{\sqrt{m}} = -\infty. \tag{6.5}$$

Proof. For each $k \geq 0$, let $c^{(k)}$ be the relation corresponding to the polynomial $p(t) = (t - f(t_0)/g(t_0))^k$ above; that is:

$$c^{(k)} = \sum_{0\leq i\leq k}(-1)^i\binom{k}{i}\left(\frac{f(t_0)}{g(t_0)}\right)^i c_{m+1+i}. \tag{6.6}$$

Thus the coefficient of $[t^j]A(t)$ in $c^{(k)}$ is

$$\alpha_j^{(k)} := -[t^{m-j}]\left(\frac{1}{h(t)}\right)t\frac{d}{dt}\left(\frac{f(t)}{g(t)}\right)(\frac{f(t)}{g(t)} - \frac{f(t_0)}{g(t_0)})^k\tilde{g}(t)^{-m}. \tag{6.7}$$

Also, define coefficients $a_j^{(k)}$ by

$$a_j^{(k)} := \frac{\alpha_j^{(k)}}{[t^{m-j}]\tilde{g}(t)^{-m}}. \tag{6.8}$$

We will consider relations of the form

$$\sum_{0\leq k\leq l}b_k m^{k/2}c^{(k)} \tag{6.9}$$

with $b_l > 0$. We first claim that for any such relation, the coefficients of $[t^j]A(t)$ are nonnegative when $j \geq Lg(t_0')n + n^{k/(k+1)}$ and n is sufficiently large. Indeed, in a neighborhood of $j/n = 1$, this follows from the estimate of Lemma 2.3; the terms for $k < l$ are $o(m^{l/2})$, while the term for $k = l$ is $\Omega(m^{l/2})$ and positive. In the other region, we use the $O(n^{-1})$ estimate of Lemma 2.4, in which the main term is positive and of order $\Omega(n^{-k/(k+1)}) > O(n^{-1})$.

In the remaining neighborhood of t_0', we use Corollary 2.5. We thus have:

$$a_{Lg(t_0')m+x\sqrt{m}}^{(k)} = C_1'(C_2')^{k+1}(C_3'm)^{-k/2}h_k(x/\sqrt{C_3'}) + o(m^{-k/2}\max(|x|^k, 1)), \tag{6.10}$$

where

$$C_1' = h(t_0')^{-1} > 0 \tag{6.11}$$

$$C_2' = -t_0'\frac{d}{dt}\left(\frac{f(t)}{g(t)}\right)_{t=t_0'} > 0 \tag{6.12}$$

$$C_3' = -t_0'Lg'(t_0') > 0. \tag{6.13}$$

23

In particular, if x is bounded above the largest zero of

$$\sum_{0 \le k \le l} b_k C_1'(C_2')^{k+1}(C_3')^{-k/2} h_k(x/\sqrt{C_3'}), \tag{6.14}$$

then we have positivity for $j \ge Lg(t_0')m + x\sqrt{m}$; when $j \le Lg(t_0')m + m^{-l/(l+1)}$, the error term is uniformly of smaller order than the main term.

Similarly,

$$a_0^{(k)} = C_1(C_2)^{k+1}(C_3 m)^{-k/2} h_k(0) + o(m^{-k/2}), \tag{6.15}$$

with

$$C_1 = h(t_0)^{-1} > 0 \tag{6.16}$$

$$C_2 = -t_0 \frac{d}{dt}\left(\frac{f(t)}{g(t)}\right)_{t=t_0} < 0 \tag{6.17}$$

$$C_3 = -t_0 Lg'(t_0) > 0. \tag{6.18}$$

Thus given any choice of b_k such that

$$q := \sum_{0 \le k \le l} b_k C_1(C_2)^{k+1}(C_3)^{-k/2} h_k(0) > 0, \tag{6.19}$$

if $x(b)$ is the largest zero of

$$p(x) := \sum_{0 \le k \le l} b_k C_1'(C_2')^{k+1}(C_3')^{-k/2} h_k(x/\sqrt{C_3'}), \tag{6.20}$$

we have the asymptotic bound

$$\limsup_{m \to \infty} \frac{d_m - Lg(t_0')m}{m^{1/2}} \le x(b). \tag{6.21}$$

To construct a good relation, we will need some further properties of the Hermite polynomials, all classical results:

Lemma 6.2. *The polynomials $h_k(x)$ are the unique monic polynomials such that*

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} h_j(x)h_k(x)e^{-x^2/2}dx = \delta_{jk}k!. \tag{6.22}$$

Furthermore, we have the three-variable generating function:

$$\sum_{k \ge 0} h_k(x)h_k(y)\frac{t^k}{k!} = \frac{1}{\sqrt{1-t^2}} \exp\left(-\frac{t^2x^2/2 - txy + t^2y^2/2}{1-t^2}\right), \tag{6.23}$$

convergent for $|t| < 1$. Finally (Christoffel-Darboux):

$$\frac{h_k(x)h_{k-1}(y) - h_{k-1}(x)h_k(y)}{x - y} = \sum_{0 \le j < k} \frac{h_j(x)h_j(y)}{j!}. \tag{6.24}$$

24

Now, given $p(x)$, we can compute b_k using orthogonality; we find:

$$b_k = \frac{1}{C_1' C_2'} \left(\frac{C_2'}{\sqrt{C_3'}} \right)^{-k} \frac{1}{\sqrt{2\pi}} \frac{1}{k!} \int p(x\sqrt{C_3'}) h_k(x) e^{-x^2/2} dx; \tag{6.25}$$

using the same formula to define b_k for $k > l$ gives $b_k = 0$. But then q can be computed as

$$\frac{C_1 C_2}{C_1' C_2'} \frac{1}{\sqrt{2\pi}} \int p(x\sqrt{C_3'}) y(x) e^{-x^2/2} dx, \tag{6.26}$$

where

$$y(x) = \sum_{0 \leq k} \left(\frac{C_2 \sqrt{C_3'}}{C_2' \sqrt{C_3}} \right)^k \frac{h_k(x) h_k(0)}{k!}. \tag{6.27}$$

Using the three-variable generating function, we find:

$$e^{-x^2/2} y(x) = e^{-x^2/2} \sum_{k \geq 0} h_k(x) h_k(y) \frac{t^k}{k!} = C^{-1} \exp(-(x/C)^2/2), \tag{6.28}$$

where

$$C := \frac{\sqrt{(C_2' \sqrt{C_3})^2 - (C_2 \sqrt{C_3'})^2}}{C_2' \sqrt{C_3}}, \tag{6.29}$$

and we must satisfy the additional requirement

$$|C_2 \sqrt{C_3'}| < |C_2' \sqrt{C_3}|, \tag{6.30}$$

precisely the additional hypothesis above. But then

$$q = \frac{C_1 C_2}{C_1' C_2'} \frac{1}{\sqrt{2\pi}} \int p(xC\sqrt{C_3'}) e^{-x^2/2} dx. \tag{6.31}$$

Since

$$\frac{C_1 C_2}{C_1' C_2'} < 0, \tag{6.32}$$

the problem reduces to the following. For an integer $k > 0$, how small can we make the largest zero of a polynomial $p(x)$ of degree $2k + 1$ subject to the condition

$$\int p(x) e^{-x^2/2} dx < 0? \tag{6.33}$$

Let $x_0^{(k)}$ be the smallest zero of $h_k(x)$, and consider the polynomials

$$p_1(x) = h_k(x) \tag{6.34}$$

$$p_2(x) = \frac{h_k(x)}{x - x_0^{(k)}}. \tag{6.35}$$

25

By Christoffel-Darboux, we compute

$$p_2(x) = h_{k-1}(x_0^{(k)})^{-1} \sum_{0 \le j < k} \frac{h_j(x)h_j(x_0^{(k)})}{j!} \tag{6.36}$$

We thus have the following integrals:

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} p_1(x)p_2(x)e^{-x^2/2}dx = 0 \tag{6.37}$$

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} p_2(x)^2 e^{-x^2/2}dx = h_{k-1}(x_0^{(k)})^{-2} \sum_{0 \le j < k} \frac{h_j(x_0^{(k)})^2}{j!} > 0. \tag{6.38}$$

Now, consider the polynomial

$$p(x) = p_1(x)p_2(x) - \epsilon p_2(x)^2 + \epsilon^2 = (x - x_0^{(k)} - \epsilon)p_2(x)^2 + \epsilon^2 \tag{6.39}$$

for $\epsilon > 0$ small. This certainly satisfies the negative integral condition; on the other hand, its only zero is that near $x_0^{(k)}$.

Thus when $l = 2k$, we obtain a bound of the form:

$$\limsup_{m \to \infty} \frac{d_m - Lg(t_0')m}{\sqrt{m}} \le C\sqrt{C_3'}x_0^{(k)}. \tag{6.40}$$

Since

$$x_0^{(k)} = -2\sqrt{k} + O(k^{-1/6}), \tag{6.41}$$

we are done. $\qquad\square$

Remark 1. The additional assumption is satisfied in all of the applications above; this is a trivial calculation for all but the lattice cases, in which it follows from the transformation law.

Remark 2. The fact that taking $2k$ coefficients gives an improvement proportional to $2\sqrt{km}$ suggests that to obtain a first-order improvement, we will need to let k grow linearly with m.

Remark 3. The involvement of the polynomial $h_k(x)^2/(x - x_0^{(k)})$ is somewhat reminiscent of the approach of Levenshtein [8] to the universa bounds, in which different orthogonal polynomials occur. There the polynomial giving the bound is

$$(p_k(x)p_{k-1}(y) - p_k(y)p_{k-1}(x))^2/(x - y), \tag{6.42}$$

which reduces to our polynomial when $p_k = h_k$ and $y = x_0^{(k)}$. While in those bounds, one lets k grow linearly with n, one can also consider finite k; in that case, the improvement is $\Omega(\sqrt{n})$, as in our case.

For the shadow cases, roughly the same argument applies; for instance, in the self-dual binary code case, we take relations starting with $m = n/12 + (\log n)^2/6$. Positivity near $j = m$ is immediate (since multiplying by a positive power series leaves positive initial coefficients positive); in the remaining region, we find that restricting

the integral to an interval $|x| \leq n^{-\epsilon}$ and replacing $(1+t)^{(\log n)^2}$ by $(1+|t|)^{(\log n)^2}$ gives negligible relative error. The argument then proceeds as before.

For the quantum cases, the difficulty is in choosing the relation. Basically, one defines $c_0^{(k)}$ and $d_0^{(k)}$ as above, and considers a linear combination of

$$m^{k/2} c_0^{(k)} \text{ and } m^{(k+1)/2}((q+1)c_0^{(k)} - (q-1)d_0^{(k)}). \tag{6.43}$$

The first set of relations has no effect on the coefficients of $[t^j]C(t) - D(t)$, so as above, we essentially obtain an arbitrary polynomial here. Similarly, they have a lower-order effect on the coefficient of $[t^0]C(t)$; we thus end up with the same constraints on this polynomial as above. On the other hand, near $j/m = Lg(t_0')$, the relations have the same order behavior; in this neighborhood, we may thus choose an arbitrary polynomial of degree $k+1$, so have no additional constraints.

References

[1] M. Aaltonen. Linear programming bounds for tree codes. *IEEE Trans. Inform. Theory*, 25(1):85–90, 1979.

[2] M. Aaltonen. A new upper bound on nonbinary block codes. *Discrete Math.*, 83(2-3):139–160, 1990.

[3] A. Ashikhmin and A. Litsyn. Upper bounds on the size of quantum codes. *IEEE Trans. Inform. Theory*, 45(4):1206–1215, 1999.

[4] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain. Type II codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, 43(3):969–976, 1997.

[5] J. H. Conway and N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory*, 36(6):1319–1332, 1990.

[6] G. A. Kabatjanskĭ and V. I. Levenštĕın. Bounds for packings on the sphere and in space. *Problems Inform. Transmission*, 14(1):1–17, 1978.

[7] I. Krasikov and S. Litsyn. An improved upper bound on the minimum distance of doubly-even self-dual codes. *IEEE Trans. Inform. Theory*, 46(1):274–278, 2000.

[8] V. I. Levenshtein. Universal bounds for codes and designs. In V. S. Pless and W. C. Huffman, editors, *Handbook of coding theory, Vol. I*, pages 499–648. North-Holland, Amsterdam, 1998.

[9] C. L. Mallows, A. M. Odlyzko, and N. J. A. Odlyzko. Upper bounds for modular forms, lattices, and codes. *J. Algebra*, 36(1):68–76, 1975.

[10] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Information and Control*, 22(2):188–200, 1973.

[11] R. J. McEliece, E. R. Rodemich, Jr. H. Rumsey, and L. R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Inform. Theory*, IT-23(2):157–166, 1977.

[12] H.-G. Quebbemann. Modular lattices in euclidean spaces. *J. Number Theory*, 54(2):190–202, October 1995.

[13] H.-G. Quebbemann. Atkin-Lehner eigenforms and strongly modular lattices. *Enseign. Math. (2)*, 43:55–65, 1997.

[14] E. Rains. Bounds for self-dual codes over Z_4. *Finite Fields Appl.*, 6(2):146–163, 2000.

[15] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44(1):134–139, 1998.

[16] E. M. Rains. Monotonicity of the quantum linear programming bound. *IEEE Trans. Inform. Theory*, 45(7):2489–2491, 1999.

[17] E. M. Rains. Quantum shadow enumerators. *IEEE Trans. Inform. Theory*, 45(7):2361–2366, 1999.

[18] E. M. Rains and N. J. A. Sloane. Self-dual codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of coding theory, Vol. I*, pages 177–294. North-Holland, Amsterdam, 1998.

[19] E. M. Rains and N. J. A. Sloane. The shadow theory of modular and unimodular lattices. *J. Number Theory*, 73(2):359–389, 1998.

[20] N. J. A. Sloane. Self-dual codes and lattices. In *Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978)*, pages 273–308. Amer. Math. Soc., 1979.