

Zeta functions for formal weight enumerators and the extremal property

By Koji CHINEN

Department of Mathematics, Faculty of Engineering, Osaka Institute of Technology, Omiya, Asahi-ku, Osaka 535-8585.
(Communicated by Shigefumi MORI, M. J. A., Dec. 12, 2005)

Abstract: In 1999, Iwan Duursma defined the zeta function for a linear code as a generating function of its Hamming weight enumerator. It has various properties similar to those of the zeta function of an algebraic curve. This article extends Duursma's theory to the case of formal weight enumerators. It is shown that the zeta function for a formal weight enumerator has a similar structure to that of the weight enumerator of a Type II code. The notion of the extremal formal weight enumerators is introduced and an analogue of the Mallows-Sloane bound is obtained. Moreover the ternary case is considered.

Key words: Zeta function for codes; formal weight enumerators; Riemann hypothesis; Mallows-Sloane bound.

1. Introduction. Let p be a prime, $q = p^r$ for some positive integer r and we denote the finite field with q elements by \mathbf{F}_q . Let C be an $[n, k, d]$ -code over \mathbf{F}_q with the Hamming weight enumerator $W_C(x, y)$. In 1999, Duursma [4] defined the zeta function for a linear code as follows:

Definition 1.1 (Duursma). For any linear code C , there exists a unique polynomial $P(T) \in \mathbf{Q}[T]$ of degree at most $n - d$ such that

$$\begin{aligned} & \frac{P(T)}{(1-T)(1-qT)} (y(1-T) + xT)^n \\ &= \dots + \frac{W_C(x, y) - x^n}{q-1} T^{n-d} + \dots \end{aligned}$$

We call $P(T)$ the zeta polynomial of the code C , and $Z(T) = P(T)/((1-T)(1-qT))$ the zeta function of C .

For a proof of existence and uniqueness of $P(T)$, the reader is referred to [1] or [2]. In his subsequent papers [5–7], Duursma deduces various interesting properties of $P(T)$ and discusses their possible applications to the coding theory. Among them, the functional equation and an analogue of the Riemann hypothesis for self-dual codes attract interests of many mathematicians, both in coding theory and number theory. When C is self-dual, the MacWilliams identity leads the functional equation of $P(T)$ of the form

$$(1) \quad P(T) = P\left(\frac{1}{qT}\right) q^g T^{2g}$$

($g = n + 1 - k - d$, see [5, p. 59]). It is the same formula as the functional equation of the zeta function of an algebraic curve (see Stichtenoth [14, Chapter V] for example), so we can formulate an analogue of the Riemann hypothesis as follows (see Duursma [6, Definition 4.1]):

Definition 1.2. The code C satisfies the Riemann hypothesis if all the zeros of $P(T)$ have the same absolute value $1/\sqrt{q}$.

One of the striking differences between the zeta functions of self-dual codes and those of algebraic curves is that the Riemann hypothesis for self-dual codes often fails to hold (in the case of the algebraic curves, the Riemann hypothesis is always true, as was proved by A. Weil). Finding an equivalent condition for a self-dual code to satisfy the Riemann hypothesis is still an open problem, but Duursma proposes the following (see [6, Open Problem 4.2])

Problem 1.3. *Prove or disprove that all extremal weight enumerators satisfy the Riemann hypothesis.*

A self-dual code C is called extremal if it has the largest possible minimum distance (see Pless [12, p. 139]). There are 4 well-known sequences of extremal self-dual codes (Types I, II, III and IV, see Conway-Sloane [3]). Duursma [7] proves that all extremal Type IV codes satisfy the Riemann hypothesis.

This article attempts to extend Duursma's theory to other classes of homogeneous polynomials than the weight enumerators of existing codes.

Studying carefully the proof of existence of $P(T)$, we notice that $W_C(x, y)$ in Definition 1.1 need not be a weight enumerator of an existing code: more essential point is that $W_C(x, y)$ is a homogeneous polynomial of the form

$$(2) \quad x^n + \sum_{i=d}^n A_i x^{n-i} y^i$$

$$(A_i \in \mathbf{C}, 1 \leq d \leq n, A_d \neq 0)$$

(see [1, p.93]). In fact, for any polynomial $W(x, y)$ of the form (2), we can similarly verify existence and uniqueness of $P(T) \in \mathbf{C}[T]$ such that

$$\frac{P(T)}{(1-T)(1-qT)}(y(1-T) + xT)^n$$

$$= \dots + \frac{W(x, y) - x^n}{q-1} T^{n-d} + \dots$$

(the number q should be determined suitably according to what meaning $W(x, y)$ has). As a class of homogeneous polynomials, we consider so-called “formal weight enumerators”:

Definition 1.4. We call $W(x, y) = \sum_{i=0}^n A_i x^{n-i} y^i \in \mathbf{C}[x, y]$ a formal weight enumerator if the following conditions are satisfied:

- (i) $A_i \neq 0 \Rightarrow 4|i$.
- (ii) $W((x+y)/\sqrt{2}, (x-y)/\sqrt{2}) = -W(x, y)$.

The notion of formal weight enumerators was first introduced by Ozeki [10] in which he deduced a remarkable result in the theory of modular forms, the construction of the Eisenstein series $E_6(z)$ using an example of formal weight enumerators and the Broué-Enguehard map. The formal weight enumerator $W(x, y)$ resembles the weight enumerators of Type II codes, but is distinguished from them by the condition (ii) of Definition 1.4 (if $W(x, y)$ is a weight enumerator of a Type II code, we have $W((x+y)/\sqrt{2}, (x-y)/\sqrt{2}) = W(x, y)$).

In this article, we establish the functional equation of the zeta polynomial of formal weight enumerators and formulate an analogue of the Riemann hypothesis. Moreover, we obtain a certain inequality similar to the Mallows-Sloane bound, which characterizes the extremal formal weight enumerators. In the last section, similar results for ternary formal weight enumerators are given.

The results in this article suggest that we should not restrict ourselves to existing linear codes when we consider “zeta functions for *linear codes*,” and that we should take into consideration various other

classes of invariant polynomials such as formal weight enumerators.

For part of the results in this paper, see also [2].

2. Zeta functions and an analogue of the Riemann hypothesis for formal weight enumerators. Let $W(x, y)$ be a formal weight enumerator and we write it in the form (2). We consider $W(x, y)$ a weight enumerator of a virtual binary self-dual code, so we set $q = 2$. Then we can determine its zeta polynomial $P(T)$. The first result is the functional equation of $P(T)$:

Theorem 2.1. *The zeta polynomial $P(T)$ of $W(x, y)$ is of degree $2g$ ($g = (n/2) + 1 - d$) and satisfies*

$$(3) \quad P(T) = -P\left(\frac{1}{2T}\right) 2^g T^{2g}.$$

Proof. The proof is similar to that of [5, p. 59] (note Definition 1.4 (ii)). □

The set of all weight enumerators of Type II codes and all formal weight enumerators forms the invariant polynomial ring $\mathbf{C}[x, y]^{G_8}$ where

$$G_8 := \left\langle \frac{1-i}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

(the group G_8 is defined in Shephard-Todd [13]). More precisely, it is known that the ring $\mathbf{C}[x, y]^{G_8}$ is generated by the following two polynomials:

$$W_8(x, y) = x^8 + 14x^4y^4 + y^8,$$

$$W_{12}(x, y) = x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12}.$$

The polynomial $W_8(x, y)$ is the weight enumerator of the extended Hamming code, a well-known example of Type II codes, and $W_{12}(x, y)$ satisfies the condition (ii) of Definition 1.4. So it follows that we found two different functional equations for the members of $\mathbf{C}[x, y]^{G_8}$:

$$P(T) = P\left(\frac{1}{2T}\right) 2^g T^{2g} \quad (\text{Type II codes}),$$

$$P(T) = -P\left(\frac{1}{2T}\right) 2^g T^{2g} \quad \left(\begin{array}{l} \text{formal weight} \\ \text{enumerators} \end{array} \right).$$

From Theorem 2.1, we can deduce that $2g$ roots of $P(T)$ are, after suitable rearrangement of them, $\alpha_1, 1/2\alpha_1, \dots, \alpha_s, 1/2\alpha_s$ for some s ($\alpha_j \neq \pm 1/\sqrt{2}$), $1/\sqrt{2}$ and $-1/\sqrt{2}$, both occur in odd multiplicity (the proof is similar to that of [14, p. 167]). So we can formulate an analogue of the Riemann hypothesis for $P(T)$ (or $W(x, y)$) in a similar way to the case of the original Duursma theory:

Definition 2.2. A formal weight enumerator $W(x, y)$ satisfies the Riemann hypothesis if all the zeros of $P(T)$ have the same absolute value $1/\sqrt{2}$.

Remark. In the cases of the zeta polynomials for algebraic curves or existing self-dual codes (over \mathbf{F}_q), the multiplicities of $\pm 1/\sqrt{q}$ are even. It is one of the different points of them from the formal weight enumerators.

In the next section, we observe closely the Riemann hypothesis and the extremal property of formal weight enumerators.

3. Extremal formal weight enumerators.

We write formal weight enumerators in the form (2).

Definition 3.1. We call a formal weight enumerator $W(x, y)$ ($\deg W = n$) “extremal” if d is the largest among all formal weight enumerators of degree n .

From the discussion of the ring $\mathbf{C}[x, y]^{G_8}$ in the previous section, we can see that the general forms of formal weight enumerators are

$$(4) \quad W_8(x, y)^l W_{12}(x, y)^{2m+1} \quad (l, m \geq 0)$$

and their suitable linear combinations (we can see formal weight enumerators $W(x, y)$ satisfy $\deg W \equiv 4 \pmod{8}$): When $\deg W \leq 28$, $W_{12}(x, y)$, $W_8(x, y)W_{12}(x, y)$ and $W_8(x, y)^2W_{12}(x, y)$ are themselves extremal, but when $\deg W \geq 36$, there always exist at least two different formal weight enumerators, so we can eliminate the terms with small powers in y :

Example 3.2. $\deg W = 36$. There are two formal weight enumerators of the form (4):

$$W_8(x, y)^3 W_{12}(x, y) = x^{36} + 9x^{32}y^4 - 828x^{28}y^8 - \dots,$$

$$W_{12}(x, y)^3 = x^{36} - 99x^{32}y^4 + 3168x^{28}y^8 - \dots$$

In this case,

$$(5) \quad \frac{11}{12}W_8(x, y)^3 W_{12}(x, y) + \frac{1}{12}W_{12}(x, y)^3$$

$$= x^{36} - 495x^{28}y^8 - 19005x^{24}y^{12} - \dots$$

is extremal. All extremal formal weight enumerators can be constructed in this way (see also [8, Chapter 19]).

We give the zeta polynomials $P_{12}(T)$, $P_{20}(T)$, $P_{28}(T)$ and $P_{36}(T)$ for $W_{12}(x, y)$, $W_8(x, y)W_{12}(x, y)W_8(x, y)^2W_{12}(x, y)$ and the polynomial (5) respectively (all these are extremal):

$$P_{12}(T) = \frac{1}{15}(2T^2 - 1)(2T^2 + 1)(2T^2 + 2T + 1),$$

$$P_{20}(T) = \frac{1}{255}(2T^2 - 1)(2T^2 + 2T + 1) \cdot (2T^2 + 1)(16T^8 + 1),$$

$$P_{28}(T) = \frac{1}{4095}(2T^2 - 1)(2T^2 + 2T + 1)(2T^2 + 1) \cdot (4T^4 - 2T^2 + 1)(4T^4 + 2T^2 + 1) \cdot (4T^4 + 4T^3 + 2T^2 + 2T + 1) \cdot (4T^4 - 4T^3 + 2T^2 - 2T + 1),$$

$$P_{36}(T) = \frac{1}{11920740}(2T^2 - 1)(199680T^{20} + 599040T^{19} + 1098240T^{18} + 1497600T^{17} + 1683904T^{16} + 1630400T^{15} + 1410176T^{14} + 1116384T^{13} + 832384T^{12} + 598544T^{11} + 424720T^{10} + 299272T^9 + 208096T^8 + 139548T^7 + 88136T^6 + 50950T^5 + 26311T^4 + 11700T^3 + 4290T^2 + 1170T + 195)$$

(we omit the zeta polynomials for others).

There seems to be a structure of the zeta functions for formal weight enumerators quite similar to that of the zeta functions for Type II codes. In fact, some computer experiments imply that extremal formal weight enumerators satisfy the Riemann hypothesis, so we may ask the following question:

Problem 3.3. *Prove or disprove that all extremal formal weight enumerators satisfy the Riemann hypothesis.*

For these observations, we proceed to investigate the extremal property of formal weight enumerators more closely. To be precise, we obtain the best possible bound for d of formal weight enumerators of the form (2):

Theorem 3.4. *For any formal weight enumerator $W(x, y)$ of the form (2), we have*

$$d \leq 4 \left\lceil \frac{n - 12}{24} \right\rceil + 4.$$

The equality holds when $W(x, y)$ is extremal.

For Type II codes, the best possible bound for the minimum distance d of extremal codes is known (see also MacWilliams-Sloane [8, pp. 624–628]):

Theorem 3.5 (Mallows-Sloane [9]). *For any Type II code of length n and minimum distance d ,*

$$d \leq 4 \left\lceil \frac{n}{24} \right\rceil + 4.$$

The equality holds in the above theorem for an extremal Type II code. We can see from the discus-

sion of Duursma [7] that Theorem 3.5 is also valid for formal weight enumerators, but it is *not the best possible*. Theorem 3.4 improves Theorem 3.5 for the case of formal weight enumerators.

Proof of Theorem 3.4. Our proof is based on the technique developed in [7, §2]. First we introduce some notations and a lemma from [7].

For a linear transformation $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we define the relation between two pairs of variables (x, y) and (u, v) as follows in accordance with [7, §2]:

$$(6) \quad (u, v) = (x, y)\sigma = (ax + cy, bx + dy).$$

We introduce the matching transformation of differential operators

$$\begin{aligned} \left(\frac{\partial}{\partial x}, \frac{\partial}{\partial y} \right) &= \left(\frac{\partial}{\partial u}, \frac{\partial}{\partial v} \right) \sigma^T \\ &= \left(a \frac{\partial}{\partial u} + b \frac{\partial}{\partial v}, c \frac{\partial}{\partial u} + d \frac{\partial}{\partial v} \right), \end{aligned}$$

where σ^T means the transposed matrix of σ .

Let $a(x, y), p(x, y)$ and $A(x, y)$ be arbitrary homogeneous polynomials over \mathbf{C} . We denote the differential operator $p(\partial/\partial x, \partial/\partial y)$ by $p(x, y)(D)$. Then we have

Lemma 3.6.

$$p((u, v)\sigma^T)(D)A(u, v) = p(x, y)(D)A((x, y)\sigma).$$

Proof. This is Lemma 1 of Duursma [7]. \square

The basic idea is that we would like to find a relation of the form

$$(7) \quad a(x, y)|p(x, y)(D)A(x, y)$$

between a (formal) weight enumerator $A(x, y)$ and some polynomials $a(x, y), p(x, y)$. Then we can say $\deg a$ is less than or equal to the degree of the right hand side. The degrees of the terms in (7) contain parameters such as the code length n and the minimum distance d . If we can find good $a(x, y)$ and $p(x, y)$, then the inequality of the degrees becomes straightforwardly a bound of d in terms of n . By this method, Duursma obtains an alternative proof of the Mallows-Sloane bounds for Types I through IV (see Theorem 3 and §1.1 of [7]). We apply this method to formal weight enumerators.

Let $W(x, y)$ be a formal weight enumerator of degree n . The number d is the same as in (2). Then we have the following two propositions:

Proposition 3.7. *If $d \geq 8$,*

$$(xy)^{d-5}(x^4 - y^4)^{d-5}|xy(x^4 - y^4)(D)W(x, y).$$

Proof. It can be shown similarly to [7, Lemma 2]. \square

Proposition 3.8. *If $d \geq 8$,*

$$(x^4 + y^4)(x^4 + 6x^2y^2 + y^4)|xy(x^4 - y^4)(D)W(x, y).$$

Proof. By definition, $W(x, y)$ can be written in the form

$$(8) \quad W(x, y) = x^n + y^n + \sum_{j=d/4}^{(n-4)/8} A_{4j} (x^{n-4j}y^{4j} + x^{4j}y^{n-4j})$$

(note that $W(y, x) = W(x, y)$ since $W(x, y)$ is invariant under G_8). Using this expression, we can easily verify

$$(x^4 + y^4)|xy(x^4 - y^4)(D)W(x, y).$$

Next we apply Lemma 3.6 with $A(x, y) = W(x, y)$, $\sigma = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $p(x, y) = xy(x^4 - y^4)$. By Definition 1.4 (ii), we have

$$\begin{aligned} p(x, y)(D)W((x, y)\sigma) &= p(x, y)(D)W(x + y, x - y) \\ &= -(\sqrt{2})^n p(x, y)(D)W(x, y). \end{aligned}$$

Since $(x^4 + y^4)|p(x, y)(D)W(x, y)$, we have

$$(u^4 + 6u^2v^2 + v^4)|p((u, v)\sigma^T)(D)W(u, v),$$

where $(u^4 + 6u^2v^2 + v^4)/8$ is the image of $x^4 + y^4$ by the transformation σ . On the other hand, we have

$$p((u, v)\sigma^T) = p(u + v, u - v) = 8p(u, v).$$

Therefore

$$(x^4 + 6x^2y^2 + y^4)|xy(x^4 - y^4)(D)W(x, y).$$

Thus we get the desired result. \square

Propositions 3.7 and 3.8 bring the following

Theorem 3.9. *For any formal weight enumerator $W(x, y)$ with $d \geq 8$, we have*

$$\begin{aligned} &(xy)^{d-5}(x^4 - y^4)^{d-5} \\ &\cdot (x^4 + y^4)(x^4 + 6x^2y^2 + y^4)|xy(x^4 - y^4)(D)W(x, y). \end{aligned}$$

Theorem 3.4 is deduced from the above theorem. Comparing the degrees in both sides of Theorem 3.9, we obtain $d \leq 4[(n - 8)/24] + 4$. Since $n = \deg W \equiv 4 \pmod{8}$, we see $[(n - 8)/24] = [(n - 12)/24]$ and get the inequality in Theorem 3.4. If $W(x, y)$ is extremal, equality holds in Theorem 3.4. This can be shown similarly to the case of Type II codes (see [8, p. 624] for example).

4. The ternary case. The same machinery exists in the case of the weight enumerators for ternary codes. In this section, we describe briefly some properties of ternary formal weight enumerators.

It is known that the Hamming weight enumerators of ternary self-dual codes belong to $\mathbf{C}[x, y]^G$ where

$$G := \left\langle \sigma_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/3} \end{pmatrix} \right\rangle.$$

The ring $\mathbf{C}[x, y]^G$ is generated by $w_4(x, y) = x^4 + 8xy^3$ and $w_{12}(x, y) = x^{12} + 264x^6y^6 + 440x^3y^9 + 24y^{12}$, the weight enumerators of the self-dual code of length 4 and the ternary Golay code, respectively ([12, p. 137]). If we take $H := \langle \sigma_1\sigma_2\sigma_1, \sigma_2 \rangle$, the subgroup of G of index 2 ([11, p. 92]), then using the generators $w_4(x, y)$ and $w_6(x, y) = x^6 - 20x^3y^3 - 8y^6$ of $\mathbf{C}[x, y]^H$, we can construct ternary formal weight enumerators. Since $w_6((x+2y)/\sqrt{3}, (x-y)/\sqrt{3}) = -w_6(x, y)$, they are of the forms

$$w_4(x, y)^l w_6(x, y)^{2m+1} \quad (l, m \geq 0)$$

and their suitable linear combinations. For the zeta polynomial $P(T)$ of a ternary formal weight enumerator $w(x, y)$ of the form (2), we have the functional equation

$$P(T) = -P\left(\frac{1}{3T}\right) 3^g T^{2g} \quad \left(g = \frac{n}{2} + 1 - d\right)$$

and similarly as in Section 2, we can formulate the Riemann hypothesis as follows:

Definition 4.1. A ternary formal weight enumerator $w(x, y)$ satisfies the Riemann hypothesis if all the zeros of $P(T)$ have the same absolute value $1/\sqrt{3}$.

Also in this case, we find a strong resemblance between zeta functions for formal weight enumerators and those for existing codes. In fact, we can observe from computer experiments that extremal ternary formal weight enumerators satisfy the Riemann hypothesis.

Here are zeta polynomials $P_6(T)$, $P_{10}(T)$, $P_{14}(T)$ and $P_{18}(T)$ for extremal ternary formal weight enumerators $w_6(x, y)$, $w_4(x, y)w_6(x, y)$, $w_4(x, y)^2w_6(x, y)$ and $(1/16)\{15w_4(x, y)^3w_6(x, y) + w_6(x, y)^3\}$ (extremal of degree 18), respectively:

$$P_6(T) = \frac{1}{2}(3T^2 - 1),$$

$$P_{10}(T) = \frac{1}{20}(3T^2 - 1)(9T^4 + 1),$$

$$P_{14}(T) = \frac{1}{182}(3T^2 - 1)(3T^2 - 3T + 1) \cdot (3T^2 + 3T + 1)(9T^4 + 3T^2 + 1),$$

$$P_{18}(T) = \frac{1}{182}(3T^2 - 1)(3T^2 + 3T + 1) \cdot (9T^4 + 3T^2 + 1)$$

(we omit the zeta polynomials for others).

We may ask a question of whether extremal ternary formal weight enumerators satisfy the Riemann hypothesis.

Acknowledgment. The author would like to express his sincere gratitude to Prof. Toyokazu Hiramatsu for giving him a chance to write a survey article [1].

References

- [1] K. Chinen and T. Hiramatsu, Zeta functions for linear codes and an analogue of the Riemann hypothesis (a survey of Iwan Duursma's work) in *Algebraic aspects of coding theory and cryptography (Kyoto, 2003)*, 91–101, RIMS Kokyuroku 1361, Kyoto, 2004. (In Japanese).
- [2] K. Chinen, Zeta functions for linear codes and an analogue of the Riemann hypothesis—a survey of Iwan Duursma's work and a generalization, in *Sendai mini symposium on number theory and combinatorial theory 2004 (Sendai, 2005)*, 31–44, Sendai, 2005. (In Japanese). <http://www.math.is.tohoku.ac.jp/~taya/sendaiNC/2004/program.html>.
- [3] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd. ed., Springer, New York, 1999.
- [4] I. M. Duursma, Weight distributions of geometric Goppa codes, *Trans. Amer. Math. Soc.* **351** (1999), no. 9, 3609–3639.
- [5] I. M. Duursma, From weight enumerators to zeta functions, *Discrete Appl. Math.* **111** (2001), no. 1–2, 55–73.
- [6] I. M. Duursma, A Riemann hypothesis analogue for self-dual codes, in *Codes and association schemes (Piscataway, NJ, 1999)*, 115–124, Amer. Math. Soc., Providence, RI.
- [7] I. M. Duursma, Extremal weight enumerators and ultraspherical polynomials, *Discrete Math.* **268** (2003), no. 1–3, 103–127.
- [8] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. I, II, North-Holland, Amsterdam, 1977.

- [9] C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Information and Control* **22** (1973), 188–200.
- [10] M. Ozeki, On the notion of Jacobi polynomials for codes, *Math. Proc. Cambridge Philos. Soc.* **121** (1997), no. 1, 15–30.
- [11] M. Ozeki, Invariant rings associated with ternary self-dual codes and their connections with Jacobi forms, in *Third spring conference “Modular forms and related topics.”* (Hamamatsu, 2004). 91–97, Ryushi-do, 2004.
- [12] V. Pless, *Introduction to the theory of error-correcting codes*, 3rd. ed., Wiley, New York, 1998.
- [13] G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canadian J. Math.* **6** (1954), 274–304.
- [14] H. Stichtenoth, *Algebraic function fields and codes*, Springer, Berlin, 1993.