Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER
Journal of Combinatorial Theory, Series A 113 (2006) 1732–1745
Journal of Combinatorial Theory
Series A
www.elsevier.com/locate/jcta

On the integrality of nth roots of generating functions

Nadia Heninger [a,1], E.M. Rains [b], N.J.A. Sloane [c]

[a] *Computer Science Department, Princeton University, Princeton, NJ 08540, USA*
[b] *Mathematics Department, University of California Davis, Davis, CA 95616, USA*
[c] *Internet and Network Systems Research Center, AT&T Shannon Labs, 180 Park Avenue, Florham Park, NJ 07932-0971, USA*

Received 13 September 2005

Available online 12 June 2006

Abstract

Motivated by the discovery that the eighth root of the theta series of the E_8 lattice and the 24th root of the theta series of the Leech lattice both have integer coefficients, we investigate the question of when an arbitrary element $f \in \mathcal{R}$ (where $\mathcal{R} = 1 + x\mathbb{Z}[\![x]\!]$) can be written as $f = g^n$ for $g \in \mathcal{R}$, $n \geqslant 2$. Let $\mathcal{P}_n := \{g^n \mid g \in \mathcal{R}\}$ and let $\mu_n := n \prod_{p \mid n} p$. We show among other things that (i) for $f \in \mathcal{R}$, $f \in \mathcal{P}_n \Leftrightarrow f \pmod{\mu_n} \in \mathcal{P}_n$, and (ii) if $f \in \mathcal{P}_n$, there is a unique $g \in \mathcal{P}_n$ with coefficients mod μ_n/n such that $f \equiv g^n \pmod{\mu_n}$. In particular, if $f \equiv 1 \pmod{\mu_n}$ then $f \in \mathcal{P}_n$. The latter assertion implies that the theta series of any extremal even unimodular lattice in $\mathbb{R}^n$ (e.g. E_8 in $\mathbb{R}^8$) is in $\mathcal{P}_n$ if n is of the form $2^i 3^j 5^k$ ($i \geqslant 3$). There do not seem to be any exact analogues for codes, although we show that the weight enumerator of the rth order Reed–Muller code of length 2^m is in $\mathcal{P}_{2^r}$ (and similarly that the theta series of the Barnes–Wall lattice BW_{2^m} is in $\mathcal{P}_{2^m}$). We give a number of other results and conjectures, and establish a conjecture of Paul D. Hanna that there is a unique element $f \in \mathcal{P}_n$ ($n \geqslant 2$) with coefficients restricted to the set $\{1, 2, \ldots, n\}$.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Formal power series; Square roots of series; Fractional powers; Integer sequences; Theta series; Barnes–Wall lattices; E_8 lattice; Leech lattice; Weight enumerators; BCH codes; Kerdock codes; Preparata codes; Reed–Muller codes

E-mail addresses: nadiah@cs.princeton.edu (N. Heninger), rains@math.ucdavis.edu (E.M. Rains), njas@research.att.com (N.J.A. Sloane).

[1] Supported by the AT&T Labs Fellowship Program.

0097-3165/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2006.03.018

1. Introduction

In June 2005, Michael Somos [36] observed that the 12th root of the theta series of Nebe's extremal 3-modular even lattice in 24 dimensions ([24,25,28], sequence A004046 in [34]) appeared to have integer coefficients. This led us to consider analogous questions for other lattices, and we discovered that the cube root of the theta series of the 6-dimensional lattice E_6, the eighth root of the theta series of the 8-dimensional lattice E_8, and the 24th root of the theta series of the 24-dimensional Leech lattice Λ_{24} also appeared to have integer coefficients. Although it seemed unlikely (and still seems unlikely!) that these results were not already known, they were new to us, and so we considered the following general question.

Let $\mathbb{Z}[\![x]\!]$ denote the ring of formal power series in x with integer coefficients, let $\mathbb{Z}[\![x]\!]^*$ denote the subset of $\mathbb{Z}[\![x]\!]$ with constant term ± 1 (that is, the set of units in $\mathbb{Z}[\![x]\!]$), and let $\mathcal{R} \subseteq \mathbb{Z}[\![x]\!]^*$ be the elements with constant term 1. If $\mathcal{P}_n$ denotes the set $\{g^n \mid g \in \mathcal{R}\}$, when is a given $f \in \mathcal{R}$ an element of $\mathcal{P}_n$ with $n \geqslant 2$?

In Section 2 we give some general conditions which ensure that a series belongs to $\mathcal{P}_n$. In Section 3 we study the theta series of lattices and establish some general theorems which explain all the above observations. We also state some conjectures which would provide converses to these theorems. Section 4 deals with the weight enumerators of codes. Surprisingly (in view of the usual parallels between self-dual codes and unimodular lattices, cf. [5,6,27]), there do not seem to be any exact analogues of the theorems for theta series. We show that the weight enumerator of the rth order Reed–Muller code of length 2^m is in $\mathcal{P}_{2^r}$ for $r = 0, 1, \ldots, m$, an make an analogous conjecture for extended BCH codes. Similarly, we show that the theta series of the Barnes–Wall lattice in $\mathbb{R}^{2^m}$ is in $\mathcal{P}_{2^m}$. In Section 5 we consider the special case of series that are squares, and report on a search for possible squares in the *On-Line Encyclopedia of Integer Sequences* [34]. This search led us to Paul Hanna's sequences, which are the subject of the final section.

It is worth mentioning that $\mathbb{Z}[\![x]\!]$ is known to be a unique factorization domain [30], although we will make no explicit use of this since we are concerned only with the multiplicative group of units in $\mathbb{Z}[\![x]\!]$.

1.1. Notation

If the formal power series $f(x) \in \mathcal{P}_n$ we will say that $f(x)$, or its sequence of coefficients, is "an nth power." For a prime p, $|\ |_p$ denotes the p-adic valuation ($|0|_p := 0$; if $0 \neq r \in \mathbb{Q}$, $r = p^a \frac{b}{c}$ with $a, b, c \in \mathbb{Z}$, $c \neq 0$, and $\gcd(p, b) = \gcd(p, c) = 1$, then $|r|_p := a$). We will use the facts that $|r!|_p < r/(p-1)$ for $r > 0$, $|\binom{p^i}{j}|_p = |p^i|_p - |j|_p$ (cf. [8]).

2. Conditions for f to be an nth power

We first show that, for investigating whether $f \in \mathcal{R}$ is an nth power, it is enough to consider $f \bmod \mu_n$, where

$$\mu_n := n \prod_{p \mid n} p.$$

Theorem 1. *For $f \in \mathcal{R}$, $f \in \mathcal{P}_n$ if and only if $f \pmod{\mu_n} \in \mathcal{P}_n$.*

Proof. We will show that, for $k \geqslant 1$, the coefficients in $f^{1/n}$ are integers if and only if the coefficients in $(f+\mu_n x^k)^{1/n}$ are integers. Let $\phi(f) := f^{1/n}$. By Taylor's theorem,

$$\begin{aligned}\phi\big(f+\mu_n x^k\big) &= \sum_{r=0}^{\infty} \frac{(\mu_n x^k)^r}{r!}\phi^{(r)}(f)\\ &= \sum_{r=0}^{\infty} \frac{(\mu_n x^k)^r}{r!} r!\binom{\frac{1}{n}}{r} f^{1/n-r}\\ &= f^{1/n}\sum_{r=0}^{\infty} \mu_n^r \binom{\frac{1}{n}}{r}\frac{x^{kr}}{f^r}.\end{aligned}$$

Let $c := \mu_n^r\binom{\frac{1}{n}}{r}$. For a prime p dividing n, $|c|_p = r|\mu_n|_p - r|n|_p - |r!|_p \geqslant 0$, by definition of μ_n. For a prime p not dividing n, $1/n$ is a p-adic unit and again $|c|_p \geqslant 0$. Hence $c \in \mathbb{Z}$. Since $f \in \mathcal{R}$, f^{-r} has integer coefficients, and so $(f+\mu_n x^k)^{1/n} = f^{1/n} g$ for some $g \in \mathcal{R}$. Thus the coefficients in $(f+\mu_n x^k)^{1/n}$ are integers if and only if the coefficients in $f^{1/n}$ are integers. □

Since $1 \in \mathcal{P}_n$, we have:

Corollary 2. *If $f \in \mathcal{R}$ satisfies $f \equiv 1 \pmod{\mu_n}$, then $f \in \mathcal{P}_n$.*

Corollary 3. *Suppose $f = 1 + f_1 x + f_2 x^2 + \cdots \in \mathcal{R}$. If A and B are positive integers such that $\mu_n \mid AB$ and $\mu_n \mid A^2$, then $f(Ax) \in \mathcal{P}_n$ if $B \mid f_1$.*

This is an immediate consequence of Corollary 2. Similar conditions involving further coefficients of f can be obtained in the same way.

For example, if $n = 2$, $f^{1/2}(4x)$ has integer coefficients for any $f \in \mathcal{R}$, and $f^{1/2}(2x)$ has integer coefficients if $2 \mid f_1$. (See Section 5 for more about the case $n = 2$.)

Furthermore, nth roots are unique mod μ_n/n:

Theorem 4. *Given $f \in \mathcal{P}_n$, there is a unique $g \in \mathcal{R} \bmod \mu_n/n$ such that $g^n \equiv f \pmod{\mu_n}$.*

Proof. Given $f \in \mathcal{P}_n$, suppose $g \in \mathcal{R}$ is such that $g^n \equiv f \pmod{\mu_n}$. We will show that, for any $k \geqslant 1$, $(g + \frac{\mu_n}{n}x^k)^n \equiv g^n \equiv f \bmod \mu_n$. In fact,

$$\left(g + \frac{\mu_n}{n}x^k\right)^n = g^n + \sum_{r=1}^{n}\binom{n}{r}\left(\frac{\mu_n}{n}\right)^r x^{rk} g^{n-r}.$$

Then for $r \geqslant 1$, $c := \binom{n}{r}(\mu_n/n)^r$ is divisible by μ_n, because for primes q not dividing n, $|c|_q = |\mu|_q = 0$, while if p divides n then $|c|_p \geqslant |n|_p - |r|_p + r \geqslant |n|_p - |r|_p + p^{|r|_p} \geqslant |\mu_n|_p = |n|_p + 1$. So we may reduce the coefficients of $g \bmod \mu_n/n$.

Conversely, suppose $g^n \equiv h^n \pmod{\mu_n}$ but $g \not\equiv h \pmod{\mu_n/n}$. Let g and h first differ at the x^k term:

$$\begin{aligned} g &= 1 + g_1 x + \cdots + g_{k-1}x^{k-1} + \alpha x^k + \cdots,\\ h &= 1 + g_1 x + \cdots + g_{k-1}x^{k-1} + \beta x^k + \cdots,\end{aligned}$$

with $\alpha \not\equiv \beta \bmod \mu_n/n$. Equating coefficients of x^k in $g^n \equiv h^n \pmod{\mu_n}$ gives $n\alpha \equiv n\beta \pmod{\mu_n}$, which implies $\alpha \equiv \beta \pmod{\mu_n/n}$, a contradiction. So g is unique. □

In the other direction, associated with any $g \in (\mathbb{Z}/\frac{\mu_n}{n}\mathbb{Z})[\![x]\!]$ with constant term 1 is a unique $f \in (\mathbb{Z}/\mu_n\mathbb{Z})[\![x]\!] \cap \mathcal{P}_n$, namely $f := g^n \bmod \mu_n$. So the elements of $\mathcal{P}_2$, for example, are enumerated by infinite binary strings beginning with 1.

We also note the following useful lemma.

Lemma 5. *For $r, s \geqslant 1$,*

$$\mathcal{P}_r \cap \mathcal{P}_s = \mathcal{P}_{\operatorname{lcm}(r,s)}.$$

Proof. Clearly $\mathcal{P}_{\operatorname{lcm}(r,s)} \subset \mathcal{P}_r, \mathcal{P}_s$. On the other hand, suppose $f \in \mathcal{P}_r \cap \mathcal{P}_s$. Let a, b be integers such that $ar + bs = \gcd(r, s)$, and define

$$g := \left(f^{\frac{1}{r}}\right)^b \left(f^{\frac{1}{s}}\right)^a.$$

Then $g \in \mathcal{R}$ and $g^{\operatorname{lcm}(r,s)} = g^{rs/\gcd(r,s)} = f$. □

3. Theta series of lattices

The theta series of an integral lattice Λ in $\mathbb{R}^d$ (that is, a lattice in which all inner products are integers) is

$$\Theta_\Lambda(x) := \sum_{u \in \Lambda} x^{u \cdot u} \in \mathcal{R}$$

The theta series of extremal lattices in various genera are especially interesting in view of their connections with modular forms and Diophantine equations [5,31,33].

Lemma 6. *If $f \in 1 + mx\mathbb{Z}[\![x]\!]$ for some integer m, then for any integer n,*

$$f^n \in 1 + mn'x\mathbb{Z}[\![x]\!],$$

where $n' = \prod_{p \mid m} p^{|n|_p}$ (or 0 if $n = 0$).

Proof. It suffices to consider the case $m = p^k$, $k > 0$, and n prime. If $n \neq p$, the claim is trivial, while otherwise, if $f = 1 + mg$, then

$$\left(f^p - 1\right)/m = \sum_{i=1}^{p} m^{i-1} \binom{p}{i} g^i.$$

Every term on the right is a multiple of p, and thus the claim follows. □

Theorem 7. *If Λ is an extremal even unimodular lattice in $\mathbb{R}^d$, d a multiple of 8, then $\Theta_\Lambda(x) \in \mathcal{P}_n$, where n is obtained from d by discarding any prime factors other than 2, 3 and 5.*

Proof. Suppose $d = 8t = 2^i 3^j 5^k 7^\ell \cdots$ (with $i \geqslant 3$), and let $a = \lfloor d/24 \rfloor = \lfloor t/3 \rfloor$. Then $n = 2^i 3^j 5^k$ and μ_n is a divisor of $30n$. It is known that $\Theta_\Lambda(x)$ can be written in the form

$$\Theta_\Lambda(x) = \sum_{i=0}^{a} c_i \psi^{t-3i}(x) \Delta^i(x), \tag{1}$$

where

$$\psi(x) := \Theta_{E_8}(x) = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) x^{2m}, \tag{2}$$

$$\Delta(x) := x^2 \prod_{m=1}^{\infty} \left(1 - x^{2m}\right)^{24}, \tag{3}$$

$\sigma_3(m)$ is the sum of the cubes of the divisors of m, and the coefficients $c_0 := 1, c_1, \ldots, c_a$ are such that

$$\Theta_\Lambda(x) = 1 + O\left(x^{2a+2}\right). \tag{4}$$

We will show that

$$\Theta_\Lambda(x) \equiv 1 \pmod{30n}, \tag{5}$$

which by Corollary 2 implies the desired result.

We apply Lemma 6, taking $f = \psi$, $m = 240$, $n = t$, $n' = 2^{i-3}3^j5^k$, obtaining $\psi^t(x) \equiv 1 \pmod{30n}$. By equating (1) and (4), we obtain an upper triangular system of equations for the c_i with diagonal entries equal to 1; this implies inductively that for $i \geqslant 1$, $c_i \equiv 0 \pmod{30n}$, and (5) follows. □

The theta series mentioned in Theorem 7 is a modular form of weight $w = d/2 \equiv 0 \bmod 4$ for the full modular group $\mathrm{SL}_2(\mathbb{Z})$. More generally, we have:

Theorem 8. *Let $f(x)$ be the extremal modular form of even weight w for $\mathrm{SL}_2(\mathbb{Z})$ (cf. [20]). Then $f(x) \in \mathcal{P}_n$, where n is obtained from $2w$ by discarding all odd primes p such that $p - 1$ does not divide w.*

Proof. To show that the extremal modular form of weight w is in $\mathcal{P}_n$, it suffices to construct *any* modular form of weight w congruent to 1 mod μ_n; this form may even have denominators, as long as they are prime to μ_n. Indeed, the difference between such a form and the extremal form will be a cusp form with all leading coefficients a multiple of μ_n; it follows as in the proof of Theorem 7 that such a cusp form has *all* coefficients a multiple of μ_n.

In particular, one may consider the Eisenstein series. Every nonconstant coefficient of E_w for w even is a multiple of $(-2w)/B_w$, where B_w is a Bernoulli number, so it suffices to show that μ_n divides the denominator of $B_w/(2w)$. By a result of Carmichael [1], m divides this denominator if and only if the exponent of $\mathbb{Z}_m^*$ divides w. In particular, 2^{k+2} divides the denominator if and only if 2^k divides w, while for odd primes, p^{k+1} divides the denominator if and only if $p^k(p-1)$ divides w. The stated rule for n follows. □

For 2- and 3-modular lattices, we take powers of Θ_{D_4} and Θ_{A_2}, respectively, to determine μ_n. Presumably these results could be improved by using the respective Eisenstein series instead.

Theorem 9. *If Λ is an extremal 2-modular lattice in $\mathbb{R}^d$, d a multiple of 4, then $\Theta_\Lambda(x) \in \mathcal{P}_n$, where n is obtained from d by discarding any prime factors other than 2 and 3.*

Theorem 10. *If Λ is an extremal 3-modular lattice in $\mathbb{R}^d$, d a multiple of 2, then $\Theta_\Lambda(x) \in \mathcal{P}_{n/2}$, where n is obtained from d by discarding any prime factors other than 2 and 3.*

It is a consequence of Theorems 7, 9 and 10 that the theta series of the following lattices are in $\mathcal{P}_d$, where d (the subscript) is the dimension of the lattice: D_4 [sequence A004011 in [34]], E_8 [A004009], BW_{16} [A008409], Λ_{24} [A008408] and Quebbemann's Q_{32} [A002272]. Also, the theta series of the Coxeter–Todd lattice K_{12} [A004010] is in $\mathcal{P}_6$, and the theta series of Nebe's 24-dimensional lattice [A004006] is in $\mathcal{P}_{12}$, establishing Somos's conjecture mentioned in Section 1. In the next section we will show more generally that the theta series of the Barnes–Wall lattice BW_{2^m} is in $\mathcal{P}_{2^m}$ for all $m \geqslant 1$.

The coefficients of the nth roots in these examples in general will not be the coefficients of any modular form (at least, not in the sense of being associated to any Fuchsian group). $\Theta_{E_8}(e^{2\pi i z})$, for example, has a zero in the open upper half-plane, and so its eighth root has an algebraic singularity in the upper half plane, and the coefficients have exponential growth.

The coefficients of the nth roots also do not appear to have any particular combinatorial significance. For example, the theta series of the D_4 lattice is

$$1 + 24x^2 + 24x^4 + 96x^6 + 24x^8 + 144x^{10} + 96x^1 + 12 + \cdots,$$

in which the coefficient of x^{2m} is the number of ways of writing $2m$ as a sum of four squares, while its fourth root [A108092] is

$$\begin{aligned} 1 &+ 6x^2 - 48x^4 + 672x^6 - 10686x^8 + 185472x^{10} - 3398304x^{12} \\ &+ 64606080x^{14} - 1261584768x^{16} + 25141699590x^{18} - 509112525600x^{20} \\ &+ 10443131883360x^{22} - 216500232587520x^{24} + 4528450460408448x^{26} \\ &- 95438941858567104x^{28} + 2024550297637849728x^{30} - \cdots. \end{aligned}$$

Do these coefficients have any other interpretation?

3.1. Further examples

The extremal *odd* unimodular lattices have been completely classified (cf. [4], [5, Chapter 19]), and the $\mathcal{P}_n$ to which their theta series belong are as follows: $\Theta_{\mathbb{Z}^d}$ $(1 \leqslant d \leqslant 7) \in \mathcal{P}_d$, $\Theta_{D_{12}^+}$ [A004533] $\in \mathcal{P}_4$, $\Theta_{E_7^{2+}}$ [A004535] $\in \mathcal{P}_2$, while the theta series of A_{15}^+ [A004536] and the odd Leech lattice [A004537] are only in $\mathcal{P}_1$. This is a straightforward verification since the theta series are known explicitly.

The theta series of both E_6 [A004007] and its dual E_6^* [A005129] are $\equiv 1 \bmod 9$ (this follows from [5, p. 127, Eqs. (121), (122)]), and so are in $\mathcal{P}_3$.

Michael Somos [36] has also pointed out that $xj(x) \in \mathcal{P}_{24}$, where $j(x)$ is the modular function $\frac{1}{x} + 744 + 196884x + \cdots$ [32]. This follows from $xj(x) = \psi(x)^3/\Delta(x)$.

We believe the value of n in Theorems 8 is best possible (and similarly for the values in Theorems 9 and 10 as far as the primes 2 and 3 are concerned). For example, it is easy to check that the theta series of the extremal even unimodular lattice in $\mathbb{R}^{56}$ [A004673] belongs to $\mathcal{P}_8$ but not $\mathcal{P}_{56}$.

The following conjecture also seems very plausible, although again we do not have a proof:

Conjecture 1. *Let $\Theta_\Lambda(x)$ be the theta series of a d-dimensional lattice. If $\Theta_\Lambda(x) \in \mathcal{P}_n$ then $n \leqslant d$. (In fact, we have not found any counterexample to the stronger conjecture that $\Theta_\Lambda(x) \in \mathcal{P}_n$ implies that n divides d.)*

Note that, considered as a formal power series, $\Theta_\Lambda(x)$ determines the dimension d (see [5, p. 47, Eq. (42)])—in Conway's terminology [3], the dimension is an "audible" property.

4. Weight enumerators of codes

The weight enumerator of an $[n, k, d]_q$ code (that is, a linear code of length n, dimension k and minimal Hamming distance d over the field $\mathbb{F}_q$) is

$$W_C(x) := \sum_{c \in C} x^{\mathrm{wt}(c)},$$

where wt denotes Hamming weight [17,19]. Although the weight enumerators are polynomials, the roots, if they exist, are normally infinite series. There does not seem to be an analogue of Theorem 7 for extremal doubly-even binary self-dual codes, since the weight enumerator of the $[24, 12, 8]_2$ Golay code,

$$1 + 759x^8 + 2576x^{12} + 759x^{16} + x^{24},$$

is not in $\mathcal{P}_n$ for any $n > 1$. However, the weight enumerator of the $[8, 4, 4]_2$ Hamming code, $1 + 14x^4 + x^8$, is in $\mathcal{P}_2$ since it is congruent to $1 + 2x^4 + x^8$ mod 4, although it is not in $\mathcal{P}_n$ for any $n > 2$.

This Hamming code is also the Reed–Muller code $RM(1, 4)$ (cf. [17,19]). More generally, we have:

Theorem 11. *Let $W_{r,m}(x)$ denote the weight enumerator of the rth order Reed–Muller code $RM(r, m)$, for $0 \leqslant r \leqslant m$, and let $W_{r,m}(x) := W_{m,m}(x) = (1 + x)^{2^m}$ for $r > m$. Then for $r \leqslant m$,*

$$W_{r,m}(x) \equiv \left(1 + x^{2^{m-r}}\right)^{2^r} \pmod{2^{r+1}}, \tag{6}$$

and so by Theorem 1 is in $\mathcal{P}_{2^r}$.

We will deduce Theorem 11 from the following result:

Theorem 12. *For $0 \leqslant r \leqslant m + 1$,*

$$W_{r,m+1}(x) - W_{r,m}\left(x^2\right) \equiv 0 \pmod{2^{m+1}}. \tag{7}$$

Proof. Reed–Muller codes may be built up recursively from

$$RM(r, m + 1) = \left\{(u, u + v) \mid u \in RM(r, m),\ v \in RM(r - 1, m)\right\}, \tag{8}$$

for $1 \leqslant r \leqslant m$, with $RM(0, m + 1) = \{0^{2^{m+1}}, 1^{2^{m+1}}\}$, $RM(m + 1, m + 1) = \{0, 1\}^{2^{m+1}}$ [19, Chapter 13, Theorem 2]. Let G be the group $(\mathbb{F}_2^+)^{m+1}$ in its natural action on $C := RM(r, m + 1)$ (consisting of the diagonal action of $(\mathbb{F}_2^+)^m$ on $RM(r, m)$ and $RM(r - 1, m)$ together with the involution swapping the two halves). If $O(x)$ is the generating function for G-orbits, indexed by the weight of the elements of the orbit, then by Burnside's lemma,

$$|G|\,O(x) = \sum_{g \in G} W_{\mathrm{Fix}_g(C)}(x),$$

where $W_{\mathrm{Fix}_g(C)}(x)$ is the weight enumerator of the subcode fixed by g. For nonzero g, $W_{\mathrm{Fix}_g(C)} = W_{r,m}(x^2)$, from (8). Therefore

$$|G|\,O(x) = W_{r,m+1}(x) + \left(|G| - 1\right) W_{r,m}\left(x^2\right).$$

Since $|G| = 2^{m+1}$, the result follows immediately. □

Theorem 11 now follows from Theorem 12 by induction on m. Another consequence of Theorem 12 is:

Corollary 13. *For any dyadic rational number* λ (*i.e., any element of* $\mathbb{Z}[1/2]$) *satisfying* $0 \leqslant \lambda \leqslant 1$, *and any integer* $r \geqslant 0$, *the sequence*

$$f_{r,m}(\lambda) = \left|\left\{u \in RM(r,m) \mid \mathrm{wt}(u) = \lambda 2^m\right\}\right|, \quad m = r, r+1, r+2, \ldots, \tag{9}$$

converges 2*-adically as* $m \to \infty$.

Special cases of this were already known, but in view of the many investigations of weight enumerators of Reed–Muller codes ([14], [15, §6.2], [19,35,37,38], etc.), it is worth putting the general remark on record. For example, in the special case $\lambda = \frac{1}{2^r}$ it follows from [19, Chapter 13, Theorem 9] that the limit in (9) is $2^r / \prod_{i=1}^{r}(1-2^i)$. Other special cases may be deduced from the results in [35] (or [19, Chapter 15, Theorem 8]) and [14].

The Nordstrom–Robinson, Kerdock and Preparata codes are closely related to Reed–Muller codes [9,16,19]. The weight enumerator of the Nordstrom–Robinson code of length 16 is in $\mathcal{P}_2$, and more generally so is that of the Kerdock code of length 4^m, $m \geqslant 2$ (this follows immediately from [19, Fig. 15.7]). It appears, although we do not have a proof, that the weight enumerator of the Preparata code of length 4^m is in $\mathcal{P}_{2^{m-3}}$.

There is a conjectural analogue of Theorem 11 for BCH codes:

Conjecture 2. *Let* C *be obtained by adding an overall parity check to the primitive BCH code of length* $2^m - 1$ *and designed distance* $2t-1$, *so that* C *has length* $n = 2^m$ *and minimal distance* $d \geqslant 2t$. *We conjecture that the weight enumerator of* C *is in* $\mathcal{P}_{2^m/d'}$, *where* d' *is the smallest power of* $2 \geqslant 2t$.

We have verified this for $m \leqslant 6$.

Here are three further examples. The Hamming weight enumerator of the $[12, 6, 6]_3$ ternary Golay code [A105683] is in $\mathcal{P}_4$, and that of the $[18, 9, 8]_4$ extremal self-dual code S_{18} over $\mathbb{F}_4$ ([2,18], A014487) is in $\mathcal{P}_{18}$. A more unlikely example is the weight enumerator of the $[48, 23, 8]_2$ Rao–Reddy code ([19,29], [A031137]),

$$\begin{aligned}
&1 + 7530x^8 + 92160x^{10} + 1080384x^{12}\\
&\quad + 7342080x^{14} + 34408911x^{16} + 111507456x^{18}\\
&\quad + 255566784x^{20} + 417404928x^{22} + 492663180x^{24}\\
&\quad + 417404928x^{26} + 255566784x^{28} + 111507456x^{30}\\
&\quad + 34408911x^{32} + 7342080x^{34} + 1080384x^{36}\\
&\quad + 92160x^{38} + 7530x^{40} + x^{48},
\end{aligned}$$

which is a square since it is congruent to $(1 + x^8 + x^{16} + x^{24})^2 \pmod 4$. (The square root is given in A108179.)

Barnes–Wall lattices are also closely related to Reed–Muller codes [5,26,27]. It will be convenient here to normalize these lattices so that the 2^m-dimensional Barnes–Wall lattice BW_{2^m} has minimal norm 2^{m-1} (making BW_{2^m} a 2^{m-1}-modular lattice, cf. [28], in which all norms are multiples of $2^{\lceil \frac{m}{2} \rceil}$). Thus the first few instances are

$$BW_2 = \mathbb{Z}^2, \quad BW_4 = D_4, \quad BW_8 = \sqrt{2}E_8, \quad BW_{16} = \sqrt{2}\Lambda_{16}, \quad \ldots.$$

Table 1

Representative	Size	Fixed sublattice
1	1	BW_{2^m}
-1	1	0
$\begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix}$	$2^{2m}+2^m-2$	$\sqrt{2}BW_{2^{m-1}}$
$\begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix}$	$2^{2m}-2^m$	0

In particular, we see that for $m = 1, \ldots, 4$, BW_{2^m} is in $\mathcal{P}_{2^m}$. In fact, we have:

Theorem 14. *The theta series of BW_{2^m} in $\mathbb{R}^{2^m}$ is congruent to* 1 (mod 2^{m+1}) *for $m \geqslant 1$, and is thus in $\mathcal{P}_{2^m}$. More precisely, for $m \geqslant 2$, we have*

$$\frac{\Theta_{BW_{2^m}}(x)-1}{2^{m+1}} \equiv \left(1-2^{m-1}\right)\frac{\Theta_{BW_{2^{m-1}}}(x^2)-1}{2^m} \pmod{2^m}. \tag{10}$$

Proof. For $m = 1$, $BW_2 = \mathbb{Z}^2$ and $\Theta_{BW_2}(x) \equiv 1 \pmod 4$. The automorphism group G of BW_{2^m} contains as a normal subgroup the extraspecial group 2_+^{1+2m} (cf. [26]). For $m \geqslant 2$ the extraspecial group consists of four conjugacy classes of G, with representatives, sizes and fixed sublattices as shown in Table 1 (here $n = 2^m$).

Then Burnside's Lemma gives us the congruence

$$\Theta_{BW_{2^m}}(x) + \left(2^{2m}-2^m+1\right) + \left(2^{2m}+2^m-2\right)\Theta_{BW_{2^{m-1}}}\left(x^2\right) \equiv 0 \pmod{2^{2m+1}},$$

which implies (10). □

This in particular implies that, for any dyadic rational $\lambda \geqslant 1$, the coefficient of $x^{\lambda 2^{m-1}}$ (that is, the number of lattice vectors of norm equal to λ times the minimal norm) in

$$\frac{\Theta_{BW_{2^m}}(x)-1}{2^{m+1}}$$

converges to a 2-adic limit. For the kissing number itself, i.e. for $\lambda = 1$, the limit is $\prod_{i=1}^{\infty}(1+2^i)$.

We end this section with a question: Is there a simple way to test if a code has a weight enumerator which is an mth power?

5. Squares

We know from Theorem 1 that to test if a given $f(x) \in \mathcal{R}$ is a square, it is enough to consider $f(x)$ mod 4, and from Theorem 4 that if $f(x)$ *is* a square then there is a unique binary series $g(x)$ associated with it. There is a simple necessary and sufficient condition for $f(x)$ to be a square.

Theorem 15. *Given $f(x) := 1 + \sum_{r \geqslant 1} f_r x^r \in \mathcal{R}$, let $\bar{f}(x) := 1 + \sum_{r \geqslant 1} \bar{f}_r x^r$ be obtained by reducing the coefficients of $f(x)$* mod 4. *If $\bar{f}_{2t} - g_t$ and $\bar{f}_{2t+1}$ are even for all $t \geqslant 0$, where $g_0 := 1, g_1, \ldots \in \mathbb{Z}/2\mathbb{Z}$ are defined recursively by*

$$\frac{\bar{f}_{2t} - g_t}{2} \equiv g_{2t} + \sum_{r=1}^{t-1} g_r g_{2t-r} \pmod 2,$$

$$\frac{\bar{f}_{2t+1}}{2} \equiv g_{2t+1} + \sum_{r=1}^{t} g_r g_{2t+1-r} \pmod 2, \tag{11}$$

then $f(x) \in \mathcal{P}_2$ *and*

$$f(x) \equiv \bar{f}(x) \equiv g^2(x) := \left(1 + \sum_{r=1}^{\infty} g_r x^r\right)^2 \pmod 4. \tag{12}$$

Conversely, if for some t *either* $\bar{f}_{2t} - g_t$ *or* $\bar{f}_{2t+1}$ *fails to be even, then* $f(x) \notin \mathcal{P}_2$.

There is a simple *necessary* condition for $f(x)$ to be a square, which generalizes to pth powers for any prime p.

Theorem 16. *Let* p *be a prime. If* $f(x) := 1 + \sum_{r \geqslant 1} f_r x^r \in \mathcal{P}_p$, *say* $f(x) = g(x)^p$, *then*

$$f_r \equiv 0 \pmod p \quad \textit{unless } p \textit{ divides } r, \tag{13}$$

$$g(x) \equiv 1 + f_p x + f_{2p} x^2 + f_{3p} x^3 + \cdots \pmod p \tag{14}$$

and

$$f(x) \equiv \left(1 + f_p x + f_{2p} x^2 + f_{3p} x^3 + \cdots\right)^p \pmod{p^2}. \tag{15}$$

Proof. This follows immediately from Theorem 4 and the fact that

$$\left(1 + g_1 x + g_2 x^2 + g_3 x^3 + \cdots\right)^p \equiv 1 + g_1 x^p + g_2 x^{2p} + g_3 x^{3p} + \cdots \pmod p. \qquad \square$$

The *On-Line Encyclopedia of Integer Sequences* [34] is a database containing over 100,000 number sequences. We tested the corresponding formal power series to see which were—or at least appeared to be—in $\mathcal{P}_2$. As a first step we used the symbolic language *Maple* [22] to weed out any series which did not begin $1 + \cdots$ or which had an obviously nonintegral square root. This produced 3030 possible members of $\mathcal{P}_2$. To reduce this number we discarded those series which appeared to be congruent to 1 mod 4, which left 905 candidates.

More detailed examination of these 905 showed that most of them could be grouped into one of the following (not necessarily disjoint) classes.

(1) Sequences which are obviously squares, usually with a square generating function. These are often described as "self-convolutions" of other sequences. For example, A008441, which gives the number of ways of writing n as the sum of two triangular numbers, with generating function $x^{-1/4}\eta(x^2)^4/\eta(x)^2$, where $\eta(x)$ is the Dedekind eta function.

(2) Sequences which reduce mod 4 to a square. For example, periodic sequences of the form

$$1, 2, 3, \ldots, k, 1, 2, 3, \ldots, k, 1, 2, 3, \ldots, k, \ldots,$$

are squares if and only if k is a multiple of 4. More generally, any sequence which reduces mod 4 to $1, 2, 3, 4, 5, 6, \ldots$ is a square.

(3) Theta series of lattices and weight enumerators of codes, as discussed in the preceding sections.

(4) McKay–Thompson series associated with conjugacy classes in the Monster simple group ([7,21], e.g., A101558). As with the modular function $j(x)$ mentioned above, the fact that these series are squares follows at once from known properties.

(5) Sequences with an exponential generating function involving trigonometric, inverse trigonometric, exponential, etc., functions. One example out of many will serve as an illustration. Vladeta Jovović's sequence A088313 [13]:

$$1, 2, 7, 36, 241, 1950, 18271, 193256, 2270017, \ldots$$

gives the number of "sets of lists" with an odd number of lists, that is, the number of partitions of $\{1, \ldots, n\}$ into an odd number of ordered subsets (cf. Motzkin [23]). There is no apparent reason why this should be a square. The analogous sequences for an even number of lists (A088312) or with any number of lists (A000292) are not squares. Jovović's sequence has exponential generating function

$$\sinh\left(\frac{x}{1-x}\right) = x + \frac{2}{2!}x^2 + \frac{7}{3!}x^3 + \frac{36}{4!}x^4 + \frac{241}{5!}x^5 + \frac{1950}{6!}x^6 + \frac{18271}{7!}x^7 + \cdots,$$

and is a square, since an elementary calculation shows that if

$$\sinh\left(\frac{x}{1-x}\right) = \sum_{k=1}^{\infty} c_k \frac{x^k}{k!},$$

then $c_k \equiv k \pmod 4$.

(6) Paul Hanna's sequences, discussed in the following section. These were the most interesting examples that were turned up by our search. We were disappointed not to find other sequences as challenging as these.

(7) Sequences whose square root proved to have a nonintegral coefficient once further terms were computed.

6. Paul Hanna's sequences

In May 2003, Paul D. Hanna [11] contributed a family of sequences to [34]. For $k \geqslant 1$, the kth Hanna sequence $H_k := (1, h_1, h_2, \ldots)$ is defined as follows: for all $n \geqslant 1$, h_n is the smallest number from the set $\{1, \ldots, k\}$ such that $(1 + h_1 x + h_2 x^2 + \cdots)^{1/k}$ has integer coefficients. He asked if the sequences are well-defined and unique for all k, and if they are eventually periodic.

For example, H_2 [A083952] is

$$1, 2, 1, 2, 2, 2, 1, 2, 2, 2, 1, 2, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 1, 2, 2, 2, 1, 2, 1, \ldots,$$

and the coefficients of its square root [A084202] are

$$1, 1, 0, 1, 0, 1, -1, 2, -2, 4, -6, 10, -16, 27, -44, 75, -127, 218, -375, 650, -1130, \ldots.$$

The sequence H_3 [A083953] is

$$1, 3, 3, 1, 3, 3, 3, 3, 3, 3, 3, 3, 1, 3, 3, 2, 3, 3, 2, 3, 3, 1, 3, 3, 2, 3, 3, 3, 3, 3, 2, 3, 3, 3, 3, \ldots,$$

and the coefficients of its cube root [A084203] are

$$1, 1, 0, 0, 1, -1, 2, -2, 2, 0, -4, 12, -24, 38, -46, 33, 29, -176, 443, -827, 1222, -1310, \ldots.$$

Theorem 17. *For all $k \geqslant 1$, H_k is well-defined and is unique.*

Proof. Suppose $f(x) := 1 + h_1 x + h_2 x^2 + \cdots = g(x)^k$, where $g(x) := 1 + g_1 x + g_2 x^2 + \cdots$. Then for $n \geqslant 1$, $h_n = k g_n + \Phi(g_1, \ldots, g_{n-1})$, for some function $\Phi(g_1, \ldots, g_{n-1})$. Write $\Phi(g_1, \ldots, g_{n-1}) = qk + r$, $0 \leqslant r < k$. If $r = 0$, $h_n = k$ and $g_n = -(q-1)$, while if $r > 0$, $h_n = r$ and $g_n = -q$. □

We will analyze H_2 and H_3 in detail, find generating functions for them, and show that they are not periodic. We know from Section 2 that to study the kth root $(H_k)^{1/k}$ it is enough to look at its values mod μ_k/k. The square root of H_2 read mod 2 gives the binary sequence

$$S_2 := (1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, \ldots)$$

[A108336], and the cube root of H_3 read mod 3 gives

$$S_3 := (1, 1, 0, 0, 1, 2, 2, 1, 2, 0, 2, 0, 0, 2, 2, 0, 2, 1, 2, 1, 1, 1, 1, 1, 0, 1, 1, \ldots)$$

[A104405].

Theorem 18. *The generating function $g(x) := 1 + x + x^3 + x^5 + x^6 + \cdots$ for S_2 satisfies $g(0) = 1$ and*

$$g\left(x^2\right) + g(x)^2 \equiv \frac{2}{1-x} \pmod 4. \tag{16}$$

Proof. If $f(x)$ is the generating function for H_2, we have $f(x) \equiv g(x)^2 \pmod 4$. It follows (compare Theorem 15) that $f_{2t} = 1$ if $g_t = 1$, $f_{2t} = 2$ if $g_t = 0$, and $f_{2t+1} = 2$. Thus $f_{2t} \equiv 3g_t + 2 \pmod 4$. Hence

$$f(x) \equiv 3g\left(x^2\right) + \frac{2}{1-x^2} + \frac{2x}{1-x^2} \pmod 4, \tag{17}$$

and (16) follows. □

Corollary 19. *H_2 is not periodic.*

Proof. H_2 is periodic if and only if S_2 is. Suppose S_2 is periodic with period π. Then $g(x) = p(x)/(1-x^\pi)$, where $p(x)$ is a polynomial of degree $\leqslant \pi - 1$. From (16),

$$\frac{p(x^2)}{1-x^{2\pi}} + \frac{p(x)^2}{(1-x^\pi)^2} \equiv \frac{2}{1-x} \pmod 4, \tag{18}$$

hence

$$p\left(x^2\right)\left(1-x^\pi\right) + p(x)^2\left(1+x^\pi\right) \equiv 2\frac{(1-x^\pi)(1-x^{2\pi})}{1-x} \pmod 4.$$

The coefficient of $x^{3\pi-1}$ is 0 on the left, 2 on the right, a contradiction. □

Similar arguments apply to the ternary case; we omit the details.

Theorem 20. *Let* $g(x) := 1 + x + x^4 + 2x^5 + 2x^6 + \cdots$ *be the generating function for* S_3*, and write it as* $g(x) = g_+(x) + 2g_-(x)$*, where* $g_+(x)$ (*respectively* $g_-(x)$) *contains the powers of* x *with coefficient* 1 (*respectively* 2)*. Then* $g(x)$ *satisfies* $g(0) = 1$ *and*

$$2g_+\left(x^3\right) + g_-\left(x^3\right) + g(x)^3 \equiv \frac{3}{1-x} \pmod 9. \tag{19}$$

The generating function for H_3 *is given by*

$$f(x) \equiv \frac{3}{1-x} - 2g_+\left(x^3\right) - g_-\left(x^3\right) \pmod 9. \tag{20}$$

Corollary 21. H_3 *is not periodic.*

We have not studied the sequences H_k for $k \geqslant 4$.

Another sequence of Hanna's is worth mentioning. This is the sequence $a_0, a_1, a_2, \ldots$ defined by $a_0 = 1$, and for $n > 0$, a_n is the smallest positive number not already in the sequence such that $(a_0 + a_1x + a_2x^2 + \cdots)^{1/3}$ has integer coefficients [A083349]:

$$1, 3, 6, 4, 9, 12, 7, 15, 18, 2, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 5, 54, 57, 10, 60, \ldots.$$

Although this sequence is similar in spirit to H_3, there is no obvious relation between them. Hanna [10] has shown that this sequence is a permutation of the positive integers. No generating function is presently known.

7. Postscript, November 6, 2005

We cannot resist adding one further example, again a sequence [A111983] studied by Paul Hanna. The series

$$f(x) := \sum_{n=0}^{\infty} (2n+1)8^n x^{\frac{n(n+1)}{2}}$$

is in $\mathcal{P}_{12}$.

Proof. Mod 9, $f(x) \equiv \sum_0^\infty (-1)^n(2n+1)x^{n(n+1)/2} = \prod_{m=1}^\infty (1-x^m)^3$, by an identity of Jacobi [12, Theorem 357], so by Theorem 1 $f(x) \in \mathcal{P}_3$. Mod 8, $f(x) \equiv 1$, so $f(x) \in \mathcal{P}_4$ by Corollary 2, and then $f(x) \in \mathcal{P}_{12}$ by Lemma 5. □

Acknowledgments

N.H. thanks the AT&T Labs Fellowship Program for support during the summer of 2005 at Florham Park, NJ, when this research was carried out. We thank Michael Somos for telling us about his discovery of the property of Nebe's lattice which prompted this work and for further discussions about theta functions of lattices. We also thank Andrew Granville for some helpful comments, and Allan Wilks for some computations related to Hanna's sequences.

References

[1] R.D. Carmichael, Note on a new number theory function, Bull. Amer. Math. Soc. 16 (1909–1910) 232–238.

[2] Y. Cheng, N.J.A. Sloane, The automorphism group of an [18, 9, 8] quaternary code, Discrete Math. 83 (1990) 205–212.
[3] J.H. Conway, The Sensual Quadratic Form, Math. Assoc. America, Washington, DC, 1997.
[4] J.H. Conway, A.M. Odlyzko, N.J.A. Sloane, Extremal self-dual lattices exist only in dimensions 1–8, 12, 14, 15, 23 and 24, Mathematika 25 (1978) 36–43.
[5] J.H. Conway, N.J.A. Sloane, Sphere Packings, Lattices and Groups, third ed., Springer-Verlag, New York, 1998.
[6] N.D. Elkies, Lattices, linear codes, and invariants, Notices Amer. Math. Soc. 47 (2000) 1238–1245 and 1382–1391.
[7] D. Ford, J. McKay, S.P. Norton, More on replicable functions, Comm. Algebra 22 (1994) 5175–5193.
[8] F.Q. Gouvêa, p-Adic Numbers, Springer-Verlag, New York, 1993.
[9] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[10] P.D. Hanna, Entries A083349 and A083350 in [34], April 2003.
[11] P.D. Hanna, Entries A083952, A084202, A083953, A084203, A083954, A084204, A083945, A084205, A083946, A084206, ... in [34], May 2003.
[12] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, third. ed., Oxford Univ. Press, 1954.
[13] V. Jovović, Entries A088312 and A088313 in [34], November 2003.
[14] T. Kasami, N. Tokura, S. Azumi, On the weight enumeration of weights less than 2.5d of Reed–Muller codes, Inform. Control 30 (1976) 380–395.
[15] J.H. van Lint, Coding Theory, Lecture Notes in Math., vol. 201, Springer-Verlag, 1971.
[16] J.H. van Lint, Kerdock codes and Preparata codes, in: Proc. Fourteenth Southeastern Conf. Combinatorics, Graph Theory, Computing, Boca Raton, FL, 1983, in: Congr. Numer., vol. 39, 1983, pp. 25–41.
[17] J.H. van Lint, Introduction to Coding Theory, third ed., Springer-Verlag, New York, 1999.
[18] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, H.N. Ward, Self-dual codes over GF(4), J. Combin. Theory Ser. A 25 (1978) 288–318.
[19] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[20] C.L. Mallows, A.M. Odlyzko, N.J.A. Sloane, Upper bounds for modular forms, lattices and codes, J. Algebra 36 (1975) 68–76.
[21] J. McKay, H. Strauss, The q-series of monstrous moonshine and the decomposition of the head characters, Comm. Algebra 18 (1990) 253–278.
[22] M.B. Monagan, et al., Maple 9 Introductory Programming Guide, Waterloo Maple Inc., Waterloo, ON, 2003.
[23] T.S. Motzkin, Sorting numbers for cylinders and other classification numbers, in: Combinatorics, in: Proc. Sympos. Pure Math., vol. 19, Amer. Math. Soc., Providence, RI, 1971, pp. 167–176.
[24] G. Nebe, Endliche Rationale Matrixgruppen vom Grad 24, Dissertation, RWTH Aachen, 1995.
[25] G. Nebe, Some cyclo-quaternionic lattices, J. Algebra 199 (1998) 472–498.
[26] G. Nebe, E.M. Rains, N.J.A. Sloane, A simple construction for the Barnes–Wall lattices, in: R.E. Blahut, R. Koetter (Eds.), Codes, Graphs and Systems: A Celebration of the Life and Career of G. David Forney, Jr. on the Occasion of his Sixtieth Birthday, Kluwer, Boston, 2002, pp. 333–342.
[27] G. Nebe, E.M. Rains, N.J.A. Sloane, Self-Dual Codes and Invariant Theory, Springer-Verlag, 2006.
[28] H.-G. Quebbemann, Modular lattices in euclidean spaces, J. Number Theory 54 (1995) 190–202.
[29] V.V. Rao, S.M. Reddy, A (48, 31, 8) linear code, IEEE Trans. Inform. Theory 19 (1973) 709–711.
[30] P. Samuel, On unique factorization domains, Illinois J. Math. 5 (1961) 1–17.
[31] R. Scharlau, R. Schulze-Pillot, Extremal lattices, in: B.H. Matzat, G.M. Greuel, G. Hiss (Eds.), Algorithmic Algebra and Number Theory, Springer-Verlag, 1999, pp. 139–170.
[32] B. Schoeneberg, Elliptic Modular Functions, Springer-Verlag, New York, 1974.
[33] J.-P. Serre, Cours d'arithmétique, third ed., Presses Universitaires de France, Paris, 1988; English translation of 1st edition published by Springer-Verlag, New York, 1977.
[34] N.J.A. Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/, 2006.
[35] N.J.A. Sloane, E.R. Berlekamp, Weight enumerator for second-order Reed–Muller code, IEEE Trans. Inform. Theory 16 (1970) 745–751.
[36] M. Somos, Personal communication, June, 2005.
[37] M. Sugino, Y. Ienaga, M. Tokura, T. Kasami, Weight distribution of (128, 64) Reed–Muller code, IEEE Trans. Inform. Theory 17 (1971) 627–628.
[38] T. Sugita, T. Kasami, T. Fujiwara, The weight distribution of the third-order Reed–Muller code of length 512, IEEE Trans. Inform. Theory 42 (1996) 1622–1625.