Chapter 9
Algebraic Quasi Cyclic Codes

9.1 Introduction

Binary self-dual codes have an interesting structure and some are known to have the best possible minimum Hamming distance of any known codes. Closely related to the self-dual codes are the double-circulant codes. Many good binary self-dual codes can be constructed in double-circulant form. Double-circulant codes as a class of codes have been the subject of a great deal of attention, probably because they include codes, or the equivalent codes, of some of the most powerful and efficient codes known to date. An interesting family of binary, double-circulant codes, which includes self-dual and formally self-dual codes, is the family of codes based on primes. A classic paper for this family was published by Karlin [9] in which double-circulant codes based on primes congruent to ± 1 and ± 3 modulo 8 were considered. Self-dual codes are an important category of codes because there are bounds on their minimal distance [**?**]. The possibilities for their weight spectrum are constrained, and known ahead of the discovery, and analysis of the codes themselves. This has created a great deal of excitement among researchers in the rush to be the first in finding some of these codes. A paper summarising the state of knowledge of these codes was given by Dougherty et al. [1]. Advances in high-speed digital processors now make it feasible to implement near maximum likelihood, soft decision decoders for these codes and thus, make it possible to approach the predictions for frame error rate (FER) performance for the additive white Gaussian noise channel made by Claude Shannon back in 1959 [16].

This chapter considers the binary double-circulant codes based on primes, especially in analysis of their Hamming weight distributions. Section 9.2 introduces the notation used to describe double-circulant codes and gives a review of double-circulant codes based on primes congruent to ± 1 and ± 3 modulo 8. Section 9.4 describes the construction of double-circulant codes for these primes and Sect. 9.5 presents an improved algorithm to compute the minimum Hamming distance and also

M. Tomlinson et al., *Error-Correction Coding and Decoding*,
Signals and Communication Technology,
DOI 10.1007/978-3-319-51103-0_9

the number of codewords of a given Hamming weight for certain double-circulant codes. The algorithm presented in this section requires the enumeration of less codewords than that of the commonly used technique [4, 18] e.g. Sect. 9.6 considers the Hamming weight distribution of the double-circulant codes based on primes. A method to provide an independent verification to the number of codewords of a given Hamming weight in these double-circulant codes is also discussed in this section. In the last section of this chapter, Sect. 9.7, a probabilistic method—based on its automorphism group, to determine the minimum Hamming distance of these double-circulant codes is described.

Note that, as we consider Hamming space only in this chapter, we shall omit the word "Hamming" when we refer to Hamming weight and distance.

9.2 Background and Notation

A code $\mathscr{C}$ is called *self-dual* if,

$$\mathscr{C} = \mathscr{C}^{\perp}$$

where $\mathscr{C}^{\perp}$ is the dual of $\mathscr{C}$. There are two types of self-dual code: *doubly even* or Type-II for which the weight of every codeword is divisible by 4; *singly even* or Type-I for which the weight of every codeword is divisible by 2. Furthermore, the code length of a Type-II code is divisible by 8. On the other hand, formally self-dual (FSD) codes are codes that have

$$\mathscr{C} \neq \mathscr{C}^{\perp},$$

but satisfy $A_{\mathscr{C}}(z) = A_{\mathscr{C}^{\perp}}(z)$, where $A(\mathscr{C})$ denotes the weight distribution of the code $\mathscr{C}$. A self-dual, or FSD, code is called *extremal* if its minimum distance is the highest possible given its parameters. The bound of the minimum distance of the extremal codes is [15]

$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4 + \varepsilon, \tag{9.1}$$

where

$$\varepsilon = \begin{cases} -2 & \text{if } \mathscr{C} \text{ is Type-I with } n = 2, 4, \text{ or } 6, \\ 2, & \text{if } \mathscr{C} \text{ is Type-I with } n \equiv 22 \pmod{24}, \text{ or} \\ 0, & \text{if } \mathscr{C} \text{ is Type-I or Type-II with } n \not\equiv 22 \pmod{24}. \end{cases} \tag{9.2}$$

for an extremal FSD code with length n and minimum distance d. For an FSD code, the minimum distance of the extremal case is upper bounded by [4]

$$d \leq 2\left\lfloor \frac{n}{8} \right\rfloor + 2. \tag{9.3}$$

As a consequence of this upper bound, extremal FSD codes are known to only exist for lengths $n \leq 30$ and $n \neq 16$ and $n \neq 26$ [7]. Databases of best-known, not necessary extremal, self-dual codes are given in [3, 15]. A table of binary self-dual double-circulant codes is also provided in [15].

As a class, double-circulant codes are (n, k) linear codes, where $k = n/2$, whose generator matrix $\boldsymbol{G}$ consists of two circulant matrices.

Definition 9.1 (*Circulant Matrix*) A circulant matrix is a square matrix in which each row is a cyclic shift of the adjacent row. In addition, each column is also a cyclic shift of the adjacent column and the number of non-zeros per column is equal to those per row.

A circulant matrix is completely characterised by a polynomial formed by its first row

$$r(x) = \sum_{i=0}^{m-1} r_i x^i,$$

which is called the *defining polynomial*.

Note that the algebra of polynomials modulo $x^m - 1$ is isomorphic to that of circulants [13]. Let the polynomial $r(x)$ have a maximum degree of m, and the corresponding circulant matrix $\boldsymbol{R}$ is an $m \times m$ square matrix of the form

$$\boldsymbol{R} = \begin{bmatrix} r(x) & (\text{mod } x^m - 1) \\ xr(x) & (\text{mod } x^m - 1) \\ & \vdots \\ x^i r(x) & (\text{mod } x^m - 1) \\ & \vdots \\ x^{m-1} r(x) & (\text{mod } x^m - 1) \end{bmatrix} \tag{9.4}$$

where the polynomial in each row can be represented by an m-dimensional vector, which contains the coefficients of the corresponding polynomial.

9.2.1 Description of Double-Circulant Codes

A double-circulant binary code is an $(n, \frac{n}{2})$ code in which the generator matrix is defined by two circulant matrices, each matrix being $\frac{n}{2}$ by $\frac{n}{2}$ bits. Circulant consists of cyclically shifted rows, modulo $\frac{n}{2}$, of a generator polynomial. These generator polynomials are defined as $r_1(x)$ and $r_2(x)$. Each codeword consists of two parts: the information data, defined as $u(x)$, convolved with $r_1(x)$ modulo $(1 + x^{\frac{n}{2}})$ adjoined with $u(x)$ and convolved with $r_2(x)$ modulo $(1 + x^{\frac{n}{2}})$. The code is the same as a non-systematic, tail-biting convolutional code of rate one

half. Each codeword is $[u(x)r_1(x), u(x)r_2(x)]$. If $r_1(x)$ [or $r_2(x)$] has no common factors of $(1 + x^{\frac{n}{2}})$, then the respective circulant matrix is non-singular and may be inverted. The inverted circulant matrix becomes an identity matrix, and each codeword is defined by $u(x), u(x)r(x)$, where $r(x) = \frac{r_1(x)}{r_2(x)}$ modulo $(1 + x^{\frac{n}{2}})$, [or $r(x) = \frac{r_2(x)}{r_1(x)}$ modulo $(1 + x^{\frac{n}{2}})$, respectively]. The code is now the same as a systematic, tail-biting convolutional code of rate one half.

For double-circulant codes where one circulant matrix is non-singular and may be inverted, the codes can be put into two classes, namely *pure*, and *bordered* double-circulant codes, whose generator matrices $\boldsymbol{G}_p$ and $\boldsymbol{G}_b$ are shown in (9.5a)

$$\boldsymbol{G}_p = \left[\begin{array}{c|c} \boldsymbol{I}_k & \boldsymbol{R} \end{array}\right] \tag{9.5a}$$

and (9.5b),

$$\boldsymbol{G}_b = \left[\begin{array}{c|c|c} & 1 \ldots 1 & \alpha \\ \hline \boldsymbol{I}_k & \boldsymbol{R} & \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \end{array}\right] \tag{9.5b}$$

respectively. Here, $\boldsymbol{I}_k$ is a k-dimensional identity matrix, and $\alpha \in \{0, 1\}$.

Definition 9.2 (*Quadratic Residues*) Let α be a generator of the finite field $\mathbb{F}_p$, where p be an odd prime, $r \equiv \alpha^2 \pmod{p}$ is called a quadratic residue modulo p and so is $r^i \in \mathbb{F}_p$ for some integer i. Because the element α has (multiplicative) order $p - 1$ over $\mathbb{F}_p$, $r = \alpha^2$ has order $\frac{1}{2}(p - 1)$. A set of quadratic residues modulo p, Q and non-quadratic residues modulo p, N, are defined as

$$\begin{aligned} Q &= \{r, r^2, \ldots, r^i, \ldots, r^{\frac{p-3}{2}}, r^{\frac{p-1}{2}} = 1\} \\ &= \{\alpha^2, \alpha^4, \ldots, \alpha^{2i} \ldots, \alpha^{p-3}, \alpha^{p-1} = 1\} \end{aligned} \tag{9.6a}$$

and

$$\begin{aligned} N &= \{n : \forall n \in \mathbb{F}_p,\ n \neq Q \text{ and } n \neq 0\} \\ &= \{nr, nr^2, \ldots, nr^i, \ldots, nr^{\frac{p-3}{2}}, n\} \\ &= \{\alpha^{2i+1} \ :\ 0 \leq i \leq \tfrac{p-3}{2}\} \end{aligned} \tag{9.6b}$$

respectively.

As such $R \cup Q \cup \{0\} = \mathbb{F}_p$. It can be seen from the definition of Q and N that, if $r \in Q$, $r = \alpha^e$ for even e; and if $n \in N$, $n = \alpha^e$ for odd e. Hence, if $n \in N$ and

$r \in Q, rn = \alpha^{2i}\alpha^{2j+1} = \alpha^{2(i+j)+1} \in N$. Similarly, $rr = \alpha^{2i}\alpha^{2j} = \alpha^{2(i+j)} \in Q$ and $nn = \alpha^{2i+1}\alpha^{2j+1} = \alpha^{2(i+j+1)} \in Q$.

Furthermore,

- $2 \in Q$ if $p \equiv \pm 1 \pmod 8$, and $2 \in N$ if $p \equiv \pm 3 \pmod 8$
- $-1 \in Q$ if $p \equiv 1 \pmod 8$ or $p \equiv -3 \pmod 8$, and $-1 \in N$ if $p \equiv -1 \pmod 8$ and $p \equiv 3 \pmod 8$

9.3 Good Double-Circulant Codes

9.3.1 Circulants Based Upon Prime Numbers Congruent to ±3 Modulo 8

An important category is circulants whose length is equal to a prime number, p, which is congruent to ± 3 modulo 8. For many of these prime numbers, there is only a single cyclotomic coset, apart from zero. In these cases, $1 + x^p$ factorises into the product of two irreducible polynomials, $(1 + x)(1 + x + x^2 + x^3 + \cdots + x^{p-1})$. Apart from the polynomial, $(1 + x + x^2 + x^3 + \cdots + x^{p-1})$, all of the other $2^p - 2$ non-zero polynomials of degree less than p are in one of two sets: The set of 2^{p-1} even weight, polynomials with $1 + x$ as a factor, denoted as $\mathbf{S_f}$, and the set of 2^{p-1} odd weight polynomials which are relatively prime to $1 + x^p$, denoted as $\mathbf{S_r}$. The multiplicative order of each set is $2^{p-1} - 1$, and each forms a ring of polynomials modulo $1 + x^p$. Any non-zero polynomial apart from $(1 + x + x^2 + x^3 + \cdots + x^{p-1})$ is equal to $\alpha(x)^i$ for some integer i if the polynomial is in $\mathbf{S_f}$ or is equal to $a(x)^i$ for some integer i if in $\mathbf{S_r}$. An example for $p = 11$ is given in Appendix "Circulant Analysis $p = 11$". In this table, $\alpha(x) = 1 + x + x^2 + x^4$ and $a(x) = 1 + x + x^3$. For these primes, as the circulant length is equal to p, the generator polynomial $r(x)$ can either contain $1 + x$ as a factor, or not contain $1 + x$ as a factor, or be equal to $(1 + x + x^2 + x^3 + \cdots + x^{p-1})$. For the last case, this is not a good choice for r(x) as the minimum codeword weight is 2, which occurs when $u(x) = 1 + x$. In this case, $r(x)u(x) = 1 + x^p = 0$ modulo $1 + x^p$ and the codeword is $[1 + x,\ 0]$, a weight of 2.

When $r(x)$ is in the ring $\mathbf{S_f}$, $u(x)r(x)$ must also be in $\mathbf{S_f}$ and therefore, be of even weight, except when $u(x) = (1 + x + x^2 + x^3 + \cdots + x^{p-1})$.

In this case $u(x)r(x) = 0$ modulo $1 + x^p$ and the codeword is $[1 + x + x^2 + x^3 + \cdots + x^{p-1}, 0]$ of weight p. When $u(x)$ has even weight, the resulting codewords are doubly even. When $u(x)$ has odd weight, the resulting codewords consist of two parts, one with odd weight and the other with even weight. The net result is the codewords that always have odd weight. Thus, there are both even and odd weight codewords when $u(x)$ is from $\mathbf{S_f}$.

When $r(x)$ is in the ring $\mathbf{S_r}$, $u(x)r(x)$ is always non-zero and is in $\mathbf{S_f}$ (even weight) only when $u(x)$ has even weight, and the resulting codewords are doubly even. When $u(x)$ has odd weight, $u(x) = a(x)^j$ and $u(x)r(x) = a(x)^j a(x)^i =$

$a(x)^{i+j}$ and hence is in the ring $\mathbf{S_f}$ and has odd weight. The resulting codewords have even weight since they consist of two parts, each with odd weight. Thus, when $r(x)$ is from $\mathbf{S_r}$ all of the codewords have even weight. Furthermore, since $r(x) = a(x)^i$, $r(x)a(x)^{2^{(p-1)}-1-i} = a(x)^{2^{(p-1)}-1} = 1$ and hence, the inverse of $r(x)$, $\frac{1}{g(x)} = a(x)^{2^{(p-1)}-1-i}$.

By constructing a table (or sampled table) of $\mathbf{S_r}$, it is very straightforward to design non-singular double-circulant codes. The minimum codeword weight of the code d_{min} cannot exceed the weight of $r(x) + 1$. Hence, the weight of $a(x)^i$ needs to be at least $d_{min} - 1$ to be considered as a candidate for $r(x)$. The weight of the inverse of $r(x)$, $a(x)^{2^{(p-1)}-1-i}$ also needs to be at least $d_{min} - 1$. For odd weight $u(x) = a(x)^j$ and $u(x)r(x) = a(x)^j a(x)^i = a(x)^{(j+i)}$. Hence, the weight of $u(x)r(x)$ can be found simply by looking up the weight of $a(x)^{i+j}$ from the table. Self-dual codes are those with $\frac{1}{r(x)} = r(x^{-1})$. With a single cyclotomic coset $2^{\frac{(p-1)}{2}} = -1$, and it follows that $a(x)^{2^{\frac{(p-1)}{2}}} = a(x^{-1})$. With $r(x) = a(x)^i$, $r(x^{-1}) = a(x)^{2^{\frac{(p-1)}{2}}i}$.

In order that $\frac{1}{r(x)} = r(x^{-1})$, it is necessary that

$$a(x)^{2^{(p-1)}-1-i} = a(x)^{2^{\frac{(p-1)}{2}}i}. \tag{9.7}$$

Equating the exponents, modulo $2^{(p-1)} - 1$, gives

$$2^{\frac{(p-1)}{2}}i = m(2^{(p-1)} - 1) - i, \tag{9.8}$$

where m is an integer. Solving for i:

$$i = \frac{m(2^{(p-1)} - 1)}{(2^{\frac{(p-1)}{2}} + 1)}. \tag{9.9}$$

Hence, the number of distinct self-dual codes is equal to $(2^{\frac{(p-1)}{2}} + 1)$.

For the example, $p = 13$ as above,

$$i = m\frac{2^{(p-1)} - 1}{2^{\frac{(p-1)}{2}} + 1} = m\frac{4095}{65} = 63m$$

and there are $2^{\frac{(p-1)}{2}} + 1 = 65$ self-dual codes for $1 \leq j \leq 65$ and these are $a(x)^{63}$, $a(x)^{126}$, $a(x)^{189}, \ldots, a(x)^{4095}$.

As p is congruent to ± 3, the set $(u(x)r(x))^{2^t}$ maps to $(u(x)r(x))$ for $t = 1 \rightarrow r$, where r is the size of the cyclotomic cosets of $2^{\frac{(p-1)}{2}} + 1$. In the case of $p = 13$ above, there are 4 cyclotomic cosets of 65, three of length 10 and one of length 2. This implies that there on 4 non-equivalent self-dual codes.

For p congruent to -3 modulo 8, $(2^{\frac{(p-1)}{2}} + 1)$ is not divisible by 3. This means that the pure double-circulant quadratic residue code is not self-dual. Since the quadratic

residue code has multiplicative order 3, this means that for p congruent to -3 modulo 8, the quadratic residue, pure double-circulant code is self-orthogonal, and $r(x) = r(x^{-1})$.

For p congruent to 3, $(2^{\frac{(p-1)}{2}} + 1)$ is divisible by 3 and the pure double-circulant quadratic residue code is self-dual. In this case, $a(x)$ has multiplicative order of $2^{(p-1)} - 1$, and $a(x)^{\frac{(2^{(p-1)}-1)}{3}}$ must have exponents equal to the quadratic residues (or non-residues). The inverse polynomial is $a(x)^{\frac{2(2^{(p-1)}-1)}{3}}$ with exponents equal to the non-residues (or residues, respectively), and defines a self-dual circulant code. As an example, for $p = 11$ as listed in Appendix "Circulant Analysis $p = 11$", $2^{(p-1)} - 1 = 1023$ and $a(x)^{341} = x + x^3 + x^4 + x^5 + x^9$, the quadratic non-residues of 11 are 1, 4, 5, 9 and 3. $a(x)^{682} = x^2 + x^6 + x^7 + x^8 + x^{10}$ corresponding to the quadratic residues: 2, 8, 10, 7 and 6 as can be seen from Appendix "Circulant Analysis $p = 11$". Section 9.4.3 discusses in more detail pure double-circulant codes for these primes.

9.3.2 *Circulants Based Upon Prime Numbers Congruent to ±1 Modulo 8: Cyclic Codes*

MacWilliams and Sloane [13] discuss the Automorphism group of the extended cyclic quadratic residue (eQR) codes and show that this includes the projective special linear group $PSL_2(p)$. They describe a procedure in which a double-circulant code may be constructed from a codeword of the eQR code. It is fairly straightforward. The projective special linear group $PSL_2(p)$ for a prime p is defined by the permutation $y \rightarrow \frac{ay+b}{cy+d}$ mod p, where the integers a, b, c, d are such that two cyclic groups of order $\frac{p+1}{2}$ are obtained. A codeword of the $(p+1, \frac{p+1}{2})$ eQR code is obtained and the non-zero coordinates of the codeword placed in each cyclic group. This splits the codeword into two cyclic parts each of which defines a circulant polynomial.

The procedure is best illustrated with an example. Let $\alpha \in \mathbb{F}_{p^2}$ be a primitive $(p^2-1)^{\text{ti}}$ root of unity; then, $\beta = \alpha^{2p-2}$ is a primitive $\frac{1}{2}(p+1)^{\text{TA}}$ root of unity since $p^2 - 1 = \frac{1}{2}(2p-2)(p-1)$. Let $\lambda = 1/(1+\beta)$ and $a = \lambda^2 - \lambda$; then, the permutation π_1 on a coordinate y is defined as

$$\pi_1 : y \mapsto \frac{y+1}{ay} \qquad \text{mod } p$$

where $\pi_1 \in \text{PSL}_2(p)$ (see Sect. 9.4.3 for the definition of $\text{PSL}_2(p)$). As an example, consider the prime $p = 23$. The permutation $\pi_1 : y \rightarrow \frac{y+1}{5y}$ mod p produces the two cyclic groups

$$(1, 5, 3, 11, 9, 13, 8, 10, 20, 17, 4, 6)$$

and

$$(2, 21, 7, 16, 12, 19, 22, 0, 23, 14, 15, 18).$$

There are 3 cyclotomic cosets for $p = 23$ as follows:

$$C_0 = \{0\}$$
$$C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}$$
$$C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}.$$

The idempotent given by C_1 may be used to define a generator polynomial, $r(x)$, which defines the (23, 12, 7) cyclic quadratic residue code:

$$r(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}. \quad (9.10)$$

Codewords of the (23, 12, 7) cyclic code are given by $u(x)r(x)$ modulo $1 + x^{23}$ and with $u(x) = 1$ the non-zero coordinates of the codeword obtained are

$$(1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12)$$

the cyclotomic coset C_1.

The extended code has an additional parity check using coordinate 23 to produce the corresponding codeword of the extended (24, 12, 8) code with the non-zero coordinates:

$$(1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12, 23).$$

Mapping these coordinates to the cyclic groups with 1 in the position, where each coordinate is in the respective cyclic group and 0 otherwise, produces

$$(1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1)$$

and

$$(1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1)$$

which define the two circulant polynomials, $r_1(x)$ and $r_2(x)$, for the (24, 12, 8) pure double-circulant code

$$r_1(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$
$$r_2(x) = 1 + x^3 + x^4 + x^8 + x^{11}. \quad (9.11)$$

The inverse of $r_1(x)$ modulo $(1 + x^{12})$ is $\psi(x)$, where

$$\psi(x) = 1 + x + x^2 + x^6 + x^7 + x^8 + x^{10},$$

and this may be used to produce an equivalent (24, 12, 8) pure double-circulant code which has the identity matrix as the first circulant

Table 9.1 Double-circulant codes mostly based upon quadratic residues of prime numbers

Prime (p)	p mod 8	Circulant codes $(2p, p)$	Circulant codes $(2p+2, p+1)$	Circulant codes $(p+1, \frac{p+1}{2})$	d_{min}
7	−1			(8, 4, 4)	4
17	1			(18, 9, 6)	6
11	3	[a](22, 11, 7) $\beta(x)$	(24, 12, 8)		8
23	−1			[a](24, 12, 8)	8
13	−3	(26, 13, 7) $b(x)$			7
31	−1			(32, 16, 8)	8
19	3	(38, 19, 8) $b(x)$			8
41	1	(82, 41, 14)		(42, 21, 10)	10
47	−1			[a](48, 24, 12)	12
29	−3	(58, 29, 11) $\beta(x)$	(60, 30, 12)		12
71	−1			(72, 36, 12)	12
				[b](72, 36, 14)	14
73	1			(74, 37, 14)	14
37	−3	(74, 37, 12) $b(x)$			12
79	−1			[a](80, 40, 16)	16
43	3	(86, 43, 16) $\beta(x)$	(88, 44, 16)		16
97	1			(98, 49, 16)	16
103	−1			[a](104, 52, 20)	20
53	−3	(106, 53, 19) $\beta(x)$	(108, 54, 20)		20
113	1			(114, 57, 16)	16
59	3	(118, 59, 19) $\beta(x)$	(120, 60, 20)		20
61	−3	(122, 61, 19) $\beta(x)$	(124, 62, 20)		20
127	−1			(128, 64, 20)	20
67	3	[a](134, 67, 23) $\beta(x)$	(136, 68, 24)		24
137	1			(138, 69, 22)	22
151	−1			(152, 76, 20)	20
83	3	(166, 83, 23) $\beta(x)$	(168, 84, 24)		24
191	−1			(192, 96, 28)	28
193	1			(194, 97, 28)	28
199	−1			[a](200, 100, 32)	32
101	−3	(202, 101, 23) $\beta(x)$	(204, 102, 24)		24
107	3	(214, 107, 23) $\beta(x)$	(216, 108, 24)		24
109	−3	(218, 109, 30) $b(x)$			30
223	−1			(224, 112, 32)	32
233	1			(234, 117, 26)	26
239	−1			(240, 120, 32)	32
241	1			(242, 121, 32?)	32?
131	3	[a](262, 131, 38?) $b(x)$			38?

[a]Codes with outstanding d_{min}

[b]Codes not based on quadratic residues

The best $(2p, p)$ circulant polynomial either contains the factor $1 + x$: $\beta(x)$ or is relatively prime to $1 + x^n$: $b(x)$

$\beta(x)$ circulants can be bordered to produce $(2p + 2, p + 1)$ circulants

$$\hat{r}_1(x) = (1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11})\psi(x) \text{ modulo } (1 + x^{12})$$
$$\hat{r}_2(x) = (1 + x^3 + x^4 + x^8 + x^{11})\psi(x) \text{ } \textit{modulo} \text{ } (1 + x^{12}).$$

After evaluating terms, the two circulant polynomials are found to be

$$\hat{r}_1(x) = 1$$
$$\hat{r}_2(x) = 1 + x + x^2 + x^4 + x^5 + x^9 + x^{11}, \tag{9.12}$$

and it can be seen that the first circulant will produce the identity matrix of dimension 12. Jenson [8] lists the circulant codes for primes $p < 200$ that can be constructed in this way. There are two cases, $p = 89$ and $p = 167$, where a systematic double-circulant construction is not possible. A non-systematic double-circulant code is possible for all cases but the existence of a systematic code depends upon one of the circulant matrices being non-singular. Apart from $p = 89$ and $p = 167$ (for $p < 200$) a systematic circulant code can always be constructed in each case.

Table 9.1 lists the best circulant codes as a function of length. Most of these codes are well known and have been previously published but not necessarily as circulant codes. Moreover, the d_{min} of some of the longer codes have only been bounded and have not been explicitly stated in the literature. Nearly, all of the best codes are codes

Table 9.2 Generator polynomials for pure double-circulant codes

Code	Circulant generator polynomial exponents
(8, 4, 4)	0, 1, 2
(24, 12, 8)	0, 1, 3, 4, 5, 6, 8
(48, 24, 12)	0, 1, 2, 3, 4, 5, 6, 8, 10, 11, 13, 14, 16, 17, 18
(80, 40, 16)	0, 1, 5, 7, 9, 10, 11, 14, 15, 19, 23, 25, 27, 30, 38
(104, 52, 20)	0, 2, 5, 7, 10, 13, 14, 17, 18, 22, 23, 25, 26, 27, 28, 37, 38, 39, 40, 41, 42, 44, 45, 46, 47, 48, 49
(122, 61, 20)	0, 1, 3, 4, 5, 9, 12, 13, 14, 15, 16, 19, 20, 22, 25, 27, 34, 36, 39, 41, 42, 45, 46, 47, 48, 49, 52, 56, 57, 58, 60
(134, 67, 23)	0, 1, 4, 6, 9, 10, 14, 15, 16, 17, 19, 21, 22, 23, 24, 25, 26, 29, 33, 35, 36, 37, 39, 40, 47, 49, 54, 55, 56, 59, 60, 62, 64, 65
(156, 78, 22)	0, 2, 3, 4, 8, 9, 11, 12, 14, 16, 17, 18, 20, 22, 24, 26, 27, 29, 33, 38, 39, 41, 42, 43, 44, 45, 46, 48, 49, 50, 52, 55, 56, 60, 64, 66, 68, 71, 72, 73, 74, 75, 77
(166, 83, 24)	1, 3, 4, 7, 9, 10, 11, 12, 16, 17, 21, 23, 25, 26, 27, 28, 29, 30, 31, 33, 36, 37, 38, 40, 41, 44, 48, 49, 51, 59, 61, 63, 64, 65, 68, 69, 70, 75, 77, 78, 81
(180, 90, 26)	0, 3, 5, 6, 7, 8, 9, 11, 12, 13, 14, 17, 18, 19, 21, 22, 23, 28, 36, 37, 41, 45, 50, 51, 53, 55, 58, 59, 60, 61, 62, 63, 67, 68, 69, 72, 75, 76, 78, 81, 82, 83, 84, 85, 88
(200, 100, 32)	0, 1, 2, 5, 6, 8, 9, 10, 11, 15, 16, 17, 18, 19, 20, 26, 27, 28, 31, 34, 35, 37, 38, 39, 42, 44, 45, 50, 51, 52, 53, 57, 58, 59, 64, 66, 67, 70, 73, 75, 76, 77, 80, 82, 85, 86, 89, 92, 93, 97, 98

based upon the two types of quadratic residue circulant codes. For codes based upon $p = \pm 3 \mod 8$, it is an open question whether a better circulant code exists than that given by the quadratic residues. For $p = \pm 1 \mod 8$, there are counter examples. For example, the (72, 36, 14) code in Table 9.1 is better than the (72, 36, 12) circulant code which is based upon the extended cyclic quadratic residue code of length 71. The circulant generator polynomial g(x) for all of the codes of Table 9.1 is given in Table 9.2.

In Table 9.1, where the best $(2p, p)$ code is given as $b(x)$, the $(2p + 2, p + 1)$ circulant code can still be constructed from $\beta(x)$ but this code has the same d_{min} as the pure, double-circulant, shorter code. For example, for the prime 109, $b(x)$ produces a double-circulant (218, 109, 30) code. The polynomial $\beta(x)$ produces a double-circulant (218, 109, 29) code, which bordered becomes a (220, 110, 30) code. It should be noted that $\beta(x)$ need not have the overall parity bit border added. In this case, a $(2p + 1, p + 1)$ code is produced but with the same d_{min} as the $\beta(x)$ code. In the latter example, a (219, 110, 29) code is produced.

9.4 Code Construction

Two binary linear codes, $\mathscr{A}$ and $\mathscr{B}$, are *equivalent* if there exists a permutation π on the coordinates of the codewords which maps the codewords of $\mathscr{A}$ onto codewords of $\mathscr{B}$. We shall write this as $\mathscr{B} = \pi(\mathscr{A})$. If π transforms $\mathscr{C}$ into itself, then we say that π fixes the code, and the set of all permutations of this kind forms the automorphism group of $\mathscr{C}$, denoted as Aut($\mathscr{C}$). MacWilliams and Sloane [13] gives some necessary but not sufficient conditions on the equivalence of double-circulant codes, which are restated for convenience in the lemma below.

Lemma 9.1 (cf. [13, Problem 7, Chap. 16]) *Let $\mathscr{A}$ and $\mathscr{B}$ be double-circulant codes with generator matrices $[\boldsymbol{I}_k|\boldsymbol{A}]$ and $[\boldsymbol{I}_k|\boldsymbol{B}]$, respectively. Let the polynomials $a(x)$ and $b(x)$ be the defining polynomials of $\boldsymbol{A}$ and $\boldsymbol{B}$. The codes $\mathscr{A}$ and $\mathscr{B}$ are equivalent if any of the following conditions holds:*

(i) $\boldsymbol{B} = \boldsymbol{A}^T$, *or*
(ii) $b(x)$ *is the reciprocal of* $a(x)$, *or*
(iii) $a(x)b(x) = 1 \pmod{x^m - 1}$, *or*
(iv) $b(x) = a(x^u)$, *where m and u are relatively prime.*

Proof

(i) We can clearly see that $b(x) = \sum_{i=0}^{m-1} a_i x^{m-i}$. It follows that $b(x) = \pi(a(x))$, where $\pi : i \to m - i \pmod m$ and hence, $\mathscr{A}$ and $\mathscr{B}$ are equivalent.
(ii) Given a polynomial $a(x)$, its reciprocal polynomial can be written as $\bar{a}(x) = \sum_{i=0}^{m-1} a_i x^{m-i-1}$. It follows that $\bar{a}(x) = \pi(a(x))$, where $\pi : i \to m - i - 1 \pmod m$.

(iii) Consider the code $\mathscr{A}$, since $b(x)$ has degree less than m, it can be one of the possible data patterns and in this case, the codeword of $\mathscr{A}$ has the form $|b(x)|1|$. Clearly, this is a permuted codeword of $\mathscr{B}$.
(iv) If $(u, m) = 1$, then $\pi : i \to iu \pmod m$ is a permutation on $\{0, 1, \ldots, m-1\}$. So $b(x) = a(x^u)$ is in the code $\pi(\mathscr{A})$.

Consider an (n, k, d) pure double-circulant code, we can see that for a given user message, represented by a polynomial $u(x)$ of degree at most $k-1$, a codeword of the double-circulant code has the form $(u(x)|u(x)r(x) \pmod{x^m - 1})$. The defining polynomial $r(x)$ characterises the resulting double-circulant code. Before the choice of $r(x)$ is discussed, consider the following lemmas and corollary.

Lemma 9.2 *Let $a(x)$ be a polynomial over $\mathbb{F}_2$ of degree at most $m-1$, i.e. $a(x) = \sum_{i=0}^{m-1} a_i x^i$ where $a_i \in \{0, 1\}$. The weight of the polynomial $(1+x)a(x) \pmod{x^m - 1}$, denoted by $\mathrm{wt}_H((1+x)a(x))$ is even.*

Proof Let $w = \mathrm{wt}_H(a(x)) = \mathrm{wt}_H(xa(x))$ and $S = \{i : a_{i+1 \bmod m} = a_i \neq 0,\ 0 \leq i \leq m-1\}$:

$$\begin{aligned}\mathrm{wt}_H((1+x)a(x)) &= \mathrm{wt}_H(a(x)) + \mathrm{wt}_H(xa(x)) - 2|S| \\ &= 2(w - |S|),\end{aligned}$$

which is even.

Lemma 9.3 *An $m \times m$ circulant matrix $\boldsymbol{R}$ with defining polynomial $r(x)$ is non-singular if and only if $r(x)$ is relatively prime to $x^m - 1$.*

Proof If $r(x)$ is not relatively prime to $x^m - 1$, i.e. GCD $(r(x), x^m - 1) = t(x)$ for some polynomial $t(x) \neq 1$, then from the extended Euclidean algorithm, it follows that, for some unique polynomials $a(x)$ and $b(x)$, $r(x)a(x) + (x^m - 1)b(x) = 0$, and therefore $\boldsymbol{R}$ is singular.

If $r(x)$ is relatively prime to $x^m - 1$, i.e. GCD $(r(x), x^m - 1) = 1$, then from the extended Euclidean algorithm, it follows that, for some unique polynomials $a(x)$ and $b(x)$, $r(x)a(x) + (x^m - 1)b(x) = 1$, which is equivalent to $r(x)a(x) = 1 \pmod{x^m - 1}$. Hence $\boldsymbol{R}$ is non-singular, being invertible with a matrix inverse whose defining polynomial is $a(x)$.

Corollary 9.1 *From Lemma 9.3,*

(i) if $\boldsymbol{R}$ is non-singular, $\boldsymbol{R}^{-1}$ is an $m \times m$ circulant matrix with defining polynomial $r(x)^{-1}$, and
(ii) the weight of $r(x)$ or $r(x)^{-1}$ is odd.

Proof The proof for the first case is obvious from the proof of Lemma 9.3. For the second case, if the weight of $r(x)$ is even then $r(x)$ is divisible by $1 + x$. Since $1 + x$ is a factor of $x^m - 1$ then $r(x)$ is not relatively prime to $x^m - 1$ and the weight of $r(x)$ is necessarily odd. The inverse of $r(x)^{-1}$ is $r(x)$ and for this to exist $r(x)^{-1}$ must be relatively prime to $x^m - 1$ and the weight of $r(x)^{-1}$ is necessarily odd.

Lemma 9.4 *Let p be an odd prime, and then*

(i) $p \mid 2^{p-1} - 1$, *and*
(ii) the integer q for $pq = 2^{p-1} - 1$ is odd.

Proof From Fermat's little theorem, we know that for any integer a and a prime p, $a^{p-1} \equiv 1 \pmod{p}$. This is equivalent to $a^{p-1} - 1 = pq$ for some integer q. Let $a = 2$, we have

$$q = \frac{2^{p-1} - 1}{p}$$

which is clearly odd since neither denominator nor numerator contains 2 as a factor.

Lemma 9.5 *Let p be a prime and $j(x) = \sum_{i=0}^{p-1} x^i$; then*

$$(1 + x)^{2^{p-1}-1} = 1 + j(x) \; mod \; (x^p - 1).$$

Proof We can write $(1 + x)^{2^{p-1}-1}$ as

$$\begin{aligned}(1 + x)^{2^{p-1}-1} &= \frac{(1 + x)^{2^{p-1}}}{1 + x} = \frac{1 + x^{2^{p-1}}}{1 + x} \\ &= \sum_{i=0}^{2^{p-1}-1} x^i.\end{aligned}$$

From Lemma 9.4, we know that the integer $q = (2^{p-1} - 1)/p$ and is odd. We can then write $\sum_{i=0}^{2^{p-1}-1} x^i$ in terms of $j(x)$ as follows:

$$\begin{aligned}\sum_{i=0}^{2^{p-1}-1} x^i = 1 + x \underbrace{\left(1 + x + \cdots + x^{p-1}\right)}_{j(x)} + x^{p+1} \underbrace{\left(1 + x + \cdots + x^{p-1}\right)}_{j(x)} + \ldots + \\ x^{(q-3)p+1} \underbrace{\left(1 + x + \cdots + x^{p-1}\right)}_{j(x)} + x^{(q-2)p+1} \underbrace{\left(1 + x + \cdots + x^{p-1}\right)}_{j(x)} + \\ x^{(q-1)p+1} \underbrace{\left(1 + x + \cdots + x^{p-1}\right)}_{j(x)} \\ = 1 + \underbrace{xj(x)(1 + x^p) + x^{2p+1} j(x)(1 + x^p) + \ldots + x^{(q-3)p+1} j(x)(1 + x^p)}_{J(x)} + \\ x^{(q-1)p+1} j(x)\end{aligned}$$

Since $(1 + x^p) \pmod{x^p - 1} = 0$ for a binary polynomial, $J(x) = 0$ and we have

$$\sum_{i=0}^{2^{p-1}-1} x^i = 1 + xx^{(q-1)p} j(x) \pmod{x^p - 1}.$$

Because $x^{ip} \pmod{x^p - 1} = 1$,

$$\begin{aligned}\sum_{i=0}^{2^{p-1}-1} x^i &= 1 + xj(x) \pmod{x^p - 1} \\ &= 1 + j(x) \pmod{x^p - 1}.\end{aligned}$$

For the rest of this chapter, we consider the bordered case only and for convenience, unless otherwise stated, we shall assume that the term double-circulant code refers to (9.5b). Furthermore, we call the double-circulant codes based on primes congruent to ± 1 modulo 8, the $[p + 1, \frac{1}{2}(p + 1), d]$ extended quadratic residue (QR) codes since these exist only for $p \equiv \pm 1 \pmod 8$.

Following Gaborone [2], we call those double-circulant codes based on primes congruent to ± 3 modulo 8 the $[2(p + 1), p + 1, d]$ quadratic double-circulant (QDC) codes, i.e. $p \equiv \pm 3 \pmod 8$.

9.4.1 *Double-Circulant Codes from Extended Quadratic Residue Codes*

The following is a summary of the extended QR codes as double-circulant codes [8, 9, 13].

Binary QR codes are cyclic codes of length p over $\mathbb{F}_2$. For a given p, there exist four QR codes:

1. $\bar{\mathscr{L}_p}, \bar{\mathscr{N}_p}$ which are equivalent and have dimension $\frac{1}{2}(p - 1)$, and
2. $\mathscr{L}_p, \mathscr{N}_p$ which are equivalent and have dimension $\frac{1}{2}(p + 1)$.

The $(p + 1, \frac{1}{2}(p + 1), d)$ extended quadratic residue code, denoted by $\hat{\mathscr{L}_p}$ (resp. $\hat{\mathscr{N}_p}$), is obtained by annexing an overall parity check to $\mathscr{L}_p$ (resp. $\mathscr{N}_p$). If $p \equiv -1 \pmod 8$, $\hat{\mathscr{L}_p}$ (resp. $\hat{\mathscr{N}_p}$) is Type-II; otherwise it is FSD.

It is well known that[1] $\mathrm{Aut}(\hat{\mathscr{L}_p})$ contains the projective special linear group denoted by $\mathrm{PSL}_2(p)$ [13]. If r is a generator of the cyclic group Q, then $\sigma : i \to \pmod p$ is a member of $\mathrm{PSL}_2(p)$. Given $n \in N$, the cycles of σ can be written as

[1] Since $\hat{\mathscr{L}_p}$ and $\hat{\mathscr{N}_p}$ are equivalent, considering either one is sufficient.

$$(\infty)(n, nr, nr^2, \ldots, nr^t)(1, r, r^2, \ldots, r^t)(0), \tag{9.13}$$

where $t = \frac{1}{2}(p-3)$. Due to this property, $\boldsymbol{G}$, the generator matrix of $\hat{\mathscr{L}_p}$ can be arranged into circulants as shown in (9.14),

$$\boldsymbol{G} = \left[\begin{array}{c|cc|c|cc|c} & \infty & n\ nr\ \ldots\ nr^{t-1} & nr^t & 1\ r\ \ldots\ r^{t-1} & r^t & 0 \\ \hline \infty & 1 & 1\ 1\ \ldots\ 1 & 1 & 1\ 1\ \ldots\ 1 & 1 & 1 \\ \beta & 0 & & & & & 1 \\ \beta r & 0 & & & & & 1 \\ \vdots & \vdots & \boldsymbol{L} & & \boldsymbol{R} & & \vdots \\ \beta r^{t-1} & 0 & & & & & 1 \\ \beta r^t & 0 & & & & & 1 \end{array}\right], \tag{9.14}$$

where $\boldsymbol{L}$ and $\boldsymbol{R}$ are $\frac{1}{2}(p-1) \times \frac{1}{2}(p-1)$ circulant matrices. The rows $\beta, \beta r, \ldots, \beta r^t$ in the above generator matrix contain $\bar{e}_\beta(x), \bar{e}_{\beta r}(x), \ldots, \bar{e}_{\beta r^t}(x)$, where $\bar{e}_i(x) = x^i e(x)$ whose coordinates are arranged in the order of (9.13). Note that (9.14) can be transformed to (9.5b) as follows:

$$\left[\begin{array}{cc} 1 & \boldsymbol{J} \\ \boldsymbol{0}^T & \boldsymbol{L}^{-1} \end{array}\right] \times \left[\begin{array}{cc|cc} 1 & \boldsymbol{J} & \boldsymbol{J} & 1 \\ \boldsymbol{0}^T & \boldsymbol{L} & \boldsymbol{R} & \boldsymbol{J}^T \end{array}\right] = \left[\begin{array}{cc|c} 1 & \boldsymbol{J} + \mathbf{w}(\boldsymbol{L}^T) & \boldsymbol{J} + \mathbf{w}(\boldsymbol{R}^T)\ \ \frac{1}{2}(p+1) \\ \boldsymbol{0}^T & \boldsymbol{I}_{\frac{1}{2}(p-1)} & \boldsymbol{L}^{-1}\boldsymbol{R}\ \ \mathbf{w}(\boldsymbol{L}^{-1})^T \end{array}\right] \tag{9.15}$$

where $\boldsymbol{J}$ is an all-ones vector and $\mathbf{w}(\boldsymbol{A}) = [\mathrm{wt}_H(\boldsymbol{A}_0) \pmod 2, \mathrm{wt}_H(\boldsymbol{A}_1) \pmod 2, \ldots]$, $\boldsymbol{A}_i$ being the ith row vector of matrix $\boldsymbol{A}$. The multiplication in (9.15) assumes that $\boldsymbol{L}^{-1}$ exists and following Corollary 9.1, $\mathrm{wt}_H(l^{-1}(x)) = \mathrm{wt}_H(l(x))$ is odd. Therefore, (9.15) becomes

$$\boldsymbol{G} = \left[\begin{array}{c|c|c} & \boldsymbol{J} + \mathbf{w}(\boldsymbol{R}^T) & \frac{1}{2}(p+1) \\ \hline \boldsymbol{I}_{\frac{1}{2}(p+1)} & \boldsymbol{L}^{-1}\boldsymbol{R} & \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \end{array}\right]. \tag{9.16}$$

In relation to (9.14), consider extended QR codes for the classes of primes:

1. $p = 8m + 1$, the idempotent $e(x) = \sum_{n \in N} x^n$ and $\beta \in N$. Following [13, Theorem 24, Chap. 16], we know that $\bar{e}_{\beta r^i}(x)$ where $\beta r^i \in N$, for $0 \le i \le t$, contains $2m+1$ quadratic residues modulo p (including 0) and $2m-1$ non-quadratic residues modulo p. As a consequence, $\mathrm{wt}_H(r(x))$ is even, implying $\mathbf{w}(\boldsymbol{R}^T) = \boldsymbol{0}$ and $r(x)$ is not invertible (cf. Corollary 9.1); and $\mathrm{wt}_H(l(x))$ is odd and $l(x)$ may be invertible over polynomial modulo $x^{\frac{1}{2}(p-1)} - 1$ (cf. Corollary 9.1). Furthermore, referring to (9.5b), we have $\alpha = \frac{1}{2}(p+1) = 4m + 1 = 1 \bmod 2$.

2. $p = 8m - 1$, the idempotent $e(x) = 1 + \sum_{n \in N} x^n$ and $\beta \in Q$. Following [13, Theorem 24, Chap. 16], if we have a set S containing 0 and $4m - 1$ non-quadratic residues modulo p, the set $\beta + S$ contains $2m + 1$ quadratic residues modulo p (including 0) and $2m - 1$ non-quadratic residues modulo p. It follows that $\bar{e}_{\beta r^i}(x)$, where $\beta r^i \in Q$, for $0 \leq i \leq t$, contains $2m$ quadratic residues modulo p (excluding 0), implying that $\boldsymbol{R}$ is singular (cf. Corollary 9.1); and $2m - 1$ non-quadratic residues modulo p, implying $\boldsymbol{L}^{-1}$ may exist (cf. Corollary 9.1). Furthermore, $\mathbf{w}(\boldsymbol{R}^T) = \mathbf{0}$ and referring to (9.5b), we have $\alpha = \frac{1}{2}(p + 1) = 4m = 0 \bmod 2$.

For many $\hat{\mathscr{L}}_p$, $\boldsymbol{L}$ is invertible and Karlin [9] has shown that $p = 73, 97, 127, 137, 241$ are the known cases where the canonical form (9.5b) cannot be obtained.

Consider the case for $p = 73$, with $\beta = 5 \in N$, we have $l(x)$, the defining polynomial of the left circulant, given by

$$l(x) = x^2 + x^3 + x^4 + x^5 + x^6 + x^{11} + x^{15} + x^{16} + x^{18} + x^{20} + x^{21} + x^{25} + x^{30} + x^{31} + x^{32} + x^{33} + x^{34}.$$

The polynomial $l(x)$ contains some irreducible factors of $x^{\frac{1}{2}(p-1)} - 1 = x^{36} - 1$, i.e. GCD $(l(x), x^{36} - 1) = 1 + x^2 + x^4$, and hence, it is not invertible. In addition to form (9.5b), $\boldsymbol{G}$ can also be transformed to (9.5a), and Jenson [8] has shown that, for $7 \leq p \leq 199$, except for $p = 89, 167$, the canonical form (9.5a) exists.

9.4.2 Pure Double-Circulant Codes for Primes ±3 Modulo 8

Recall that $\mathbf{S_r}$ is a multiplicative group of order $2^{p-1} - 1$ containing all polynomials of odd weight (excluding the all-ones polynomial) of degree at most $p - 1$, where p is a prime. We assume that $a(x)$ is a generator of $\mathbf{S_r}$. For $p \equiv \pm 3 \pmod 8$, we have the following lemma.

Lemma 9.6 *For $p \equiv \pm 3 \pmod 8$, let the polynomials $q(x) = \sum_{i \in Q} x^i$ and $n(x) = \sum_{i \in N} x^i$. Self-dual pure double-circulant codes with $r(x) = q(x)$ or $r(x) = n(x)$ exist if and only if $p \equiv 3 \pmod 8$.*

Proof For self-dual codes the condition $q(x)^T = n(x)$ must be satisfied where $q(x)^T = q(x^{-1}) = \sum_{i \in Q} x^{-i}$. Let $r(x) = q(x)$, for the case when $p \equiv \pm 3 \pmod 8$, $2 \in N$ we have $q(x)^2 = \sum_{i \in Q} x^{2i} = n(x)$. We know that $1 + q(x) + n(x) = j(x)$, therefore, $q(x)^3 = q(x)^2 q(x) = n(x)q(x) = (1 + q(x) + j(x))q(x) = q(x) + n(x) + j(x) = 1$. Then, $\frac{q(x)^2}{q(x)^3} = q(x)^2$ and $q(x)^2 = n(x) = q(x)^{-1} = q(x^{-1})$. On the other hand, $-1 \in N$ if $p \equiv 3 \pmod 8$ and thus $q(x)^T = n(x)$. If $p \equiv -3 \pmod 8$, $-1 \in Q$, we have $q(x)^T = q(x)$. For $r(x) = n(x)$, the same arguments follow.

Let $\mathscr{P}_p$ denote a $(2p, p, d)$ pure double-circulant code for $p \equiv \pm 3 \pmod 8$. The properties of $\mathscr{P}_p$ can be summarised as follows:

1. For $p \equiv 3 \pmod 8$, since $q(x)^3 = 1$ and $a^{2^{p-1}-1} = 1$, we have $q(x) = a(x)^{(2^{p-1}-1)/3}$ and $q(x)^T = a(x)^{(2^p-2)/3}$. There are two full-rank generator matrices with mutually disjoint information sets associated with $\mathscr{P}_p$ for these primes. Let $\boldsymbol{G}_1$ be a reduced echelon generator matrix of $\mathscr{P}_p$, which has the form of (9.5a) with $\boldsymbol{R} = \boldsymbol{B}$, where $\boldsymbol{B}$ is a circulant matrix with defining polynomial $b(x) = q(x)$. The other full-rank generator matrix $\boldsymbol{G}_2$ can be obtained as follows:

$$\boldsymbol{G}_2 = \boxed{\boldsymbol{B}^T} \times \boldsymbol{G}_1 = \boxed{\boldsymbol{B}^T \mid \boldsymbol{I}_p}. \tag{9.17}$$

   The self-duality of this pure double-circulant code is obvious from $\boldsymbol{G}_2$.
2. For $p \equiv -3 \pmod 8$, $(p-1)/2$ is even and hence, neither $q(x)$ nor $n(x)$ is invertible, which means that if this polynomial was chosen as the defining polynomial for $\mathscr{P}_p$, there exists only one full-rank generator matrix. However, either $1 + q(x)$ (resp. $1 + n(x)$) is invertible and the inverse is $1 + n(x)$ (resp. $1 + q(x)$), i.e.

$$\begin{aligned}(1 + q(x))(1 + n(x)) &= 1 + q(x) + n(x) + q(x)n(x)\\ &= 1 + q(x) + n(x) + q(x)(1 + j(x) + q(x))\\ &= 1 + q(x) + n(x) + q(x) + q(x)j(x) + q(x)^2,\end{aligned}$$

   and since $q(x)j(x) = 0$ and $q(x)^2 = n(x)$ under polynomial modulo $x^p - 1$, it follows that

$$(1 + q(x))(1 + n(x)) = 1 \pmod{x^p - 1}.$$

   Let $\boldsymbol{G}_1$ be the first reduced echelon generator matrix, which has the form of (9.5a) where $\boldsymbol{R} = \boldsymbol{I}_p + \boldsymbol{Q}$. The other full-rank generator matrix with disjoint information sets $\boldsymbol{G}_2$ can be obtained as follows:

$$\boldsymbol{G}_2 = \boxed{\boldsymbol{I}_p + \boldsymbol{N}} \times \boldsymbol{G}_1 = \boxed{\boldsymbol{I}_p + \boldsymbol{N} \mid \boldsymbol{I}_p}. \tag{9.18}$$

   Since $-1 \in Q$ for this prime, $(\boldsymbol{I}_p + \boldsymbol{Q})^T = \boldsymbol{I}_p + \boldsymbol{Q}$ implying that the $(2p, p, d)$ pure double-circulant code is FSD, i.e. the generator matrix of $\mathscr{P}_p^{\perp}$ is given by

$$\boldsymbol{G}^{\perp} = \boxed{\boldsymbol{I}_p + \boldsymbol{Q} \mid \boldsymbol{I}_p}.$$

A bordered double-circulant construction based on these primes—commonly known as the *quadratic double-circulant* construction—also exists, see Sect. 9.4.3 below.

9.4.3 Quadratic Double-Circulant Codes

Let p be a prime that is congruent to ± 3 modulo 8. A $(2(p+1), p+1, d)$ binary quadratic double-circulant code, denoted by $\mathscr{B}_p$, can be constructed using the defining polynomial

$$b(x) = \begin{cases} 1 + q(x) & \text{if } p \equiv 3 \pmod 8, \text{ and} \\ q(x) & \text{if } p \equiv -3 \pmod 8 \end{cases} \tag{9.19}$$

where $q(x) = \sum_{i \in Q} x^i$. Following [13], the generator matrix $\boldsymbol{G}$ of $\mathscr{B}_p$ is

$$\boldsymbol{G} = \begin{array}{c|c|c|c} l_\infty & l_0 \ldots l_{p-1} & r_\infty & r_0 \ldots r_{p-1} \\ \hline 1 \\ \vdots & \boldsymbol{I}_p & 0 \\ \vdots & & \vdots & \boldsymbol{B} \\ 1 & & 0 & \\ \hline 0 & 0 \ldots 0 & 1 & 1 \ldots 1 \end{array} \tag{9.20}$$

which is, if the last row of $\boldsymbol{G}$ is rearranged as the first row, the columns indexed by l_∞ and r_∞ are rearranged as the last and the first columns, respectively, equivalent to (9.5b) with $\alpha = 0$ and $k = p + 1$. Let $j(x) = 1 + x + x^2 + \cdots + x^{p-1}$, and the following are some properties of $\mathscr{B}_p$ [9]:

1. for $p \equiv 3 \pmod 8$, $b(x)^3 = (1 + q(x))^2(1 + q(x)) = (1 + n(x))(1 + q(x)) = 1 + j(x)$, since $q(x)^2 = n(x)$ ($2 \in N$ for this prime) and $q(x)j(x) = n(x)j(x) = j(x)$ ($\mathrm{wt}_H(q(x)) = \mathrm{wt}_H(n(x))$ is odd). Also, $(b(x) + j(x))^3 = (1 + q(x) + j(x))^2(1 + q(x) + j(x)) = n(x)^2(1 + q(x) + j(x)) = q(x) + n(x) + j(x) = 1$ because $n(x)^2 = q(x)$. Since $-1 \in N$ and we have $b(x)^T = 1 + \sum_{i \in Q} x^{-i} = 1 + n(x)$ and thus, $b(x)b(x)^T = (1 + q(x))(1 + n(x)) = 1 + j(x)$.
   There are two generator full-rank matrices with disjoint information sets for $\mathscr{B}_p$. This is because, although $b(x)$ has no inverse, $b(x) + j(x)$ does, and the inverse is $(b(x) + j(x))^2$.
   Let $\boldsymbol{G}_1$ has the form of (9.5b) where $\boldsymbol{R} = \boldsymbol{B}$, and the other full-rank generator matrix $\boldsymbol{G}_2$ can be obtained as follows:

$$\boldsymbol{G}_2 = \left[\begin{array}{c|c} 1 & 1 \ \ldots \ 1 \\ \hline 0 & \\ \vdots & \boldsymbol{B}^T \\ 0 & \end{array}\right] \times \boldsymbol{G}_1 = \left[\begin{array}{c|c|c|c} 0 & 1 \ \ldots \ 1 & 1 & 0 \ \ldots \ 0 \\ \hline 1 & & 0 & \\ \vdots & \boldsymbol{B}^T & \vdots & \boldsymbol{I}_p \\ 1 & & 0 & \end{array}\right]. \tag{9.21}$$

It is obvious that $\boldsymbol{G}_2$ is identical to the generator matrix of $\mathscr{B}_p^{\perp}$ and hence, it is self-dual.

2. for $p \equiv -3 \pmod 8$, $b(x)^3 = n(x)q(x) = (1 + j(x) + q(x))q(x) = 1 + j(x)$ since $q(x)^2 = n(x)$ ($2 \in N$ for this prime) and $q(x)j(x) = n(x)j(x) = 0$ ($\mathrm{wt}_H(q(x)) = \mathrm{wt}_H(n(x))$ is even). Also, $(b(x) + j(x))^3 = (q(x) + j(x))^2(1 + n(x)) = q(x)^2 + q(x)^2 n(x) + j(x)^2 + j(x)^2 n(x) = n(x) + q(x) + j(x) = 1$ because $n(x)^2 = q(x)$. Since $-1 \in Q$ and we have $b(x)^T = \sum_{i \in Q} x^{-i} = b(x)$ and it follows that $\mathscr{B}_p$ is FSD, i.e. the generator matrix of $\mathscr{B}_p^{\perp}$ is given by

$$\boldsymbol{G}^{\perp} = \left[\begin{array}{c|c|c|c} 0 & 1 \ \ldots \ 1 & 1 & 0 \ \ldots \ 0 \\ \hline 1 & & 0 & \\ \vdots & \boldsymbol{B} & \vdots & \boldsymbol{I}_p \\ 1 & & 0 & \end{array}\right]$$

Since $(b(x) + j(x))^{-1} = (b(x) + j(x))^2$, there exist full-rank two generator matrices of disjoint information sets for $\mathscr{B}_p$. Let $\boldsymbol{G}_1$ has the form of (9.5b) where $\boldsymbol{R} = \boldsymbol{B}$, and the other full-rank generator matrix $\boldsymbol{G}_2$ can be obtained as follows:

$$\boldsymbol{G}_2 = \left[\begin{array}{c|c} 1 & 1 \ \ldots \ 1 \\ \hline 0 & \\ \vdots & \boldsymbol{B}^2 \\ 0 & \end{array}\right] \times \boldsymbol{G}_1 = \left[\begin{array}{c|c|c|c} 0 & 1 \ \ldots \ 1 & 1 & 0 \ \ldots \ 0 \\ \hline 1 & & 0 & \\ \vdots & \boldsymbol{B}^2 & \vdots & \boldsymbol{I}_p \\ 1 & & 0 & \end{array}\right] \tag{9.22}$$

Codes of the form $\mathscr{B}_p$ form an interesting family of double-circulant codes. In terms of self-dual codes, the family contains the longest extremal Type-II code known, $n = 136$. Probably, it is the longest extremal code that exists, see Sect. 9.7. Moreover, $\mathscr{B}_p$ is the binary image of the extended QR code over $\mathbb{F}_4$ [10].

The $(p + 1, \frac{1}{2}(p + 1), d)$ double-circulant codes for $p \equiv \pm 1 \pmod 8$ are fixed by $\mathrm{PSL}_2(p)$, see Sect. 9.4.1. This linear group $\mathrm{PSL}_2(p)$ is generated by the set of all permutations to the coordinates $(\infty, 0, 1, \ldots, p - 1)$ of the form

$$y \to \frac{ay + b}{cy + d}, \tag{9.23}$$

where $a, b, c, d \in \mathbb{F}_p$, $ad - bc = 1$, $y \in \mathbb{F}_p \cup \{\infty\}$, and it is assumed that $\pm\frac{1}{0} = \infty$ and $\pm\frac{1}{\infty} = 0$ in the arithmetic operations.

We know from [13] that this form of permutation is generated by the following transformations:

$$\begin{aligned} S &: y \to y+1 \\ V &: y \to \alpha^2 y \\ T &: y \to -\frac{1}{y}, \end{aligned} \tag{9.24}$$

where α is a primitive element of $\mathbb{F}_p$. In fact, V is redundant since it can be obtained from S and T, i.e.

$$V = TS^{\alpha}TS^{\mu}TS^{\alpha} \tag{9.25}$$

for[2] $\mu = \alpha^{-1} \in \mathbb{F}_p$.

The linear group $\mathrm{PSL}_2(p)$ fixes not only the $(p+1, \frac{1}{2}(p+1), d)$ binary double-circulant codes, for $p \equiv \pm 1 \pmod 8$, but also the $(2(p+1), p+1, d)$ binary quadratic double-circulant codes, as shown as follows. Consider the coordinates $(\infty, 0, 1, \ldots, p-1)$ of a circulant, the transformation S leaves the coordinate ∞ invariant and introduces a cyclic shift to the rest of the coordinates and hence S fixes a circulant. Let $\boldsymbol{R}_i$ and $\boldsymbol{L}_i$ denote the ith row of the right and left circulants of (9.20), respectively (we assume that the index starts with 0), and let $\boldsymbol{J}$ and $\boldsymbol{J}'$ denote the last row of the right and left circulant of (9.20), respectively.

Consider the primes $p = 8m+3$, $\boldsymbol{R}_0 = \left(0 \mid 1 + \sum_{i \in Q} x^i\right)$. Let e_i and f_j, for some integers i and j, be even and odd integers, respectively. If $i \in Q$, $-1/i = -1 \times \alpha^{p-1}/\alpha^{e_1} = \alpha^{f_1} \times \alpha^{e_2 - e_1} \in N$ since $-1 \in N$ for these primes. Therefore, the transformation T interchanges residues to non-residues and vice versa. In addition, we also know that T interchanges coordinates ∞ and 0. Applying transformation T to $\boldsymbol{R}_0$, $T(\boldsymbol{R}_0)$, results in

$$T(\boldsymbol{R}_0) = \left(1 \mid \sum_{j \in N} x^j\right) = \boldsymbol{R}_0 + \boldsymbol{J}.$$

Similarly, for the first row of $\boldsymbol{L}$, which has 1 at coordinates ∞ and 0 only, i.e. $\boldsymbol{L}_0 = (1 \mid 1)$

$$T(\boldsymbol{L}_0) = \boldsymbol{L}_0 + \boldsymbol{J}.$$

[2] $TS^{\alpha}TS^{\mu}TS^{\alpha}(y) = TS^{\alpha}TS^{\mu}T(y+\alpha) = TS^{\alpha}TS^{\mu}(-y^{-1}+\alpha) = TS^{\alpha}T\left(-\frac{1}{y+\mu}+\alpha\right) = TS^{\alpha}T\left(\frac{\alpha y+\alpha\mu-1}{y+\mu}\right) = TS^{\alpha}\left(\frac{-\alpha y^{-1}+\alpha\mu-1}{-y^{-1}+\mu}\right) = T\left(\frac{-\alpha(y+\alpha)^{-1}+\alpha\mu-1}{-(y+\alpha)^{-1}+\mu}\right) = T\left(\frac{(\alpha\mu-1)y+\alpha(\alpha\mu-1)-\alpha}{\mu y+(\alpha\mu-1)}\right) = \left(\frac{(-\alpha\mu-1)y^{-1}+\alpha(\alpha\mu-1)-\alpha}{-\mu y^{-1}+(\alpha\mu-1)}\right) = \left(\frac{-\alpha}{-\mu y^{-1}}\right) = \alpha^2 y = V(y)$.

Let $s \in Q$ and let the set $\hat{Q} = Q \cup \{0\}$, $\boldsymbol{R}_s = \left(0 \mid \sum_{i \in \hat{Q}} x^{s+i}\right)$ and $T\left(\sum_{i \in \hat{Q}} x^{s+i}\right) = \sum_{i \in \hat{Q}} x^{-1/(s+i)}$. Following MacWilliams and Sloane [13, Theorem 24, Chap. 16], we know that the exponents of $\sum_{i \in \hat{Q}} x^{s+i}$ contain $2m+1$ residues and $2m+1$ non-residues. Note that $s+i$ produces no 0.[3] It follows that $-1/(s+i)$ contains $2m+1$ non-residues and $2m+1$ residues. Now consider $\boldsymbol{R}_{-1/s} = \left(0 \mid \sum_{i \in \hat{Q}} x^{i-1/s}\right)$, $i - 1/s$ contains[4] 0 $i, s \in Q$, $2m$ residues and $2m+1$ non-residues. We can write $-1/(s+i)$ as

$$-\frac{1}{s+i} = \frac{i/s}{s+i} - \frac{1}{s} = z - \frac{1}{s}.$$

Let $I \subset \hat{Q}$ be a set of all residues such that for all $i \in I$, $i - 1/s \in N$. If $-1/(s+i) \in N$, $z \in \hat{Q}$ and we can see that z must belong to I such that $z - 1/s \in N$. This means these non-residues cancel each other in $T(\boldsymbol{R}_s) + \boldsymbol{R}_{-1/s}$. On the other hand, if $-1/(s+i) \in Q$, $z \in N$ and it is obvious that $z - 1/s \neq i - 1/s$ for all $i \in \hat{Q}$, implying that all $2m+1$ residues in $T(\boldsymbol{R}_s)$ are disjoint from all $2m+1$ residues (including 0) in $\boldsymbol{R}_{-1/s}$. Therefore, $T(\boldsymbol{R}_s) + \boldsymbol{R}_{-1/s} = \left(0 \mid \sum_{i \in \hat{Q}} x^i\right)$, i.e.

$$T(\boldsymbol{R}_s) = \boldsymbol{R}_{-1/s} + \boldsymbol{R}_0.$$

Similarly, $T(\boldsymbol{L}_s) = \left(0 \mid 1 + x^{-1/s}\right)$ and $\boldsymbol{L}_{-1/s} = \left(1 \mid x^{-1/s}\right)$, which means

$$T(\boldsymbol{L}_s) = \boldsymbol{L}_{-1/s} + \boldsymbol{L}_0.$$

Let $t \in N$, $\boldsymbol{R}_t = \left(0 \mid \sum_{i \in \hat{Q}} x^{t+i}\right)$ and $T\left(\sum_{i \in \hat{Q}} x^{t+i}\right) = \sum_{i \in \hat{Q}} x^{-1/(t+i)}$. We know that $t+i$ contains 0, $2m$ residues and $2m+1$ non-residues [13, Theorem 24, Chap. 16], and correspondingly $-1/(t+i)$ contains ∞, $2m$ non-residues and $2m+1$ residues. As before, now consider $\boldsymbol{R}_{-1/t} = \left(0 \mid \sum_{i \in \hat{Q}} x^{i-1/t}\right)$. There are $2m+1$ residues (excluding 0) and $2m+1$ non-residues in $i - 1/t$, and let $I' \subset \hat{Q}$ be a set of all residues such that, for all $i \in I'$, $i - 1/t \in Q$. As before, we can write $-1/(t+i)$ as $z - 1/t$, where $z = (i/t)/(t+i)$. If $-1/(t+i) \in Q$, $z \in I'$ and hence, the $2m+1$ residues from $-1/(t+i)$ are identical to those from $i - 1/t$. If $-1/(t+i) \in N$, $z \in N$ and hence, all of the $2m$ non-residues of $-1/(t+i)$ are disjoint from all $2m+1$ non-residues of $i - 1/t$. Therefore, $T(\boldsymbol{R}_t) + R_{-1/t} = \left(1 \mid \sum_{i \in N} x^i\right)$, i.e.

$$T(\boldsymbol{R}_t) = \boldsymbol{R}_{-1/t} + \boldsymbol{R}_0 + \boldsymbol{J}.$$

[3] Consider a prime $p = \pm 3 \pmod 8$, $q \in Q$ and an integer a where $(a, p) = 1$. In order for $q + a = 0$ to happen, $a = -q$. The integer a is a residue if $p = 8m - 3$ and a non-residue if $p = 8m + 3$.

[4] This is because all $i \in Q$ are considered and $1/s \in Q$.

Similarly, $T(\boldsymbol{L}_t) = \left(0 \mid 1 + x^{-1/t}\right)$ and $\boldsymbol{L}_{-1/t} = \left(1 \mid x^{-1/t}\right)$, which means

$$T(\boldsymbol{L}_t) = \boldsymbol{L}_{-1/t} + \boldsymbol{L}_0 + \boldsymbol{J}'.$$

For primes $p = 8m - 3$, $\boldsymbol{R}_0 = \left(0 \mid \sum_{i \in Q} x^i\right)$ and since $-1 \in Q$, $-1/i \in Q$ for $i \in Q$. Thus,

$$T(\boldsymbol{R}_0) = \left(0 \mid \sum_{i \in Q} x^{-1/i}\right) = \boldsymbol{R}_0.$$

Similarly, for $\boldsymbol{L}_0$, which contains 1 at coordinates 0 and ∞,

$$T\left(\boldsymbol{L}_0\right) = \boldsymbol{L}_0.$$

Consider $\boldsymbol{R}_s = \left(0 \mid \sum_{i \in Q} x^{s+i}\right)$, for $s \in Q, T\left(\sum_{i \in Q} x^{s+i}\right) = \sum_{i \in Q} x^{-1/(s+i)}$. There are 0 (when $i = -s \in Q$), $2m - 2$ residues and $2m - 1$ non-residues in the set $s + i$ [13, Theorem 24, Chap. 16]. Correspondingly, $-1/(s + i) = z - 1/s$, where $z = (i/s)/(s + i)$, contains ∞, $2m - 2$ residues and $2m - 1$ non-residues. Now consider $\boldsymbol{R}_{-1/s} = \left(0 \mid \sum_{i \in Q} x^{i-1/s}\right)$, the set $i - 1/s$ contains 0 (when $i = 1/s \in Q$), $2m - 2$ residues and $2m - 1$ non-residues. Let $I \subset Q$ be a set of all residues such that for all $i \in I$, $i - 1/s \in Q$. If $-1/(s + i) \in Q$ then $z - 1/s \in Q$ which means $z \in Q$ and z must belong to I. This means all $2m - 2$ residues of $-1/(s + i)$ and those of $i - 1/s$ are identical. On the contrary, if $-1/(s + i) \in N$, $z \in N$ and this means $z - 1/s \neq i - 1/s$ for all $i \in Q$, and therefore all non-residues in $-1/(s + i)$ and $i - 1/s$ are mutually disjoint. Thus, $T(\boldsymbol{R}_s) + \boldsymbol{R}_{-1/s} = \left(1 \mid 1 + \sum_{i \in N} x^i\right)$, i.e.

$$T(\boldsymbol{R}_s) = \boldsymbol{R}_{-1/s} + \boldsymbol{R}_0 + \boldsymbol{J}.$$

Similarly, $T(\boldsymbol{L}_s) = \left(0 \mid 1 + x^{-1/s}\right)$, and we can write

$$T(\boldsymbol{L}_s) = \boldsymbol{L}_{-1/s} + \boldsymbol{L}_0 + \boldsymbol{J}'.$$

For $t \in N$, we have $\boldsymbol{R}_t = \left(0 \mid \sum_{i \in Q} x^{t+i}\right)$ and $T(\sum_{i \in Q} x^{t+i}) = \sum_{i \in Q} x^{-1/(t+i)}$. Following [13, Theorem 24, Chap. 16], there are $2m - 1$ residues and $2m - 1$ non-residues in the set $t + i$ and the same distributions are contained in the set $-1/(t + i)$. Considering $\boldsymbol{R}_{-1/t} = \left(0 \mid \sum_{i \in Q} x^{i-1/t}\right)$, there are $2m - 1$ residues and $2m - 1$ non-residues in $i - 1/t$. Rewriting $-1/(t + i) = z - 1/t$, for $z = (i/t)/(t + i)$, and letting $I' \subset Q$ be a set of all residues such that for all $i \in I'$, $i - 1/t \in N$, we know that if $-1/(t + i) \in N$ then $z - 1/t \in N$ which means that $z \in Q$ and z must belong to I'. Hence, the non-residues in $i - 1/t$ and $-1/(t + i)$ are identical. If $-1/(t + i) \in Q$, however, $z \in N$ and for all $i \in Q$, $i - 1/t \neq z - 1/t$, implying that the residues in $-1/(t + i)$ and $i - 1/t$ are mutually disjoint. Thus, $T(\boldsymbol{R}_t) + \boldsymbol{R}_{-1/t} = \left(0 \mid \sum_{i \in Q} x^i\right)$, i.e.

$$T(\boldsymbol{R}_t) = \boldsymbol{R}_{-1/t} + \boldsymbol{R}_0.$$

Similarly, $T(\boldsymbol{L}_t) = \left(0 \mid 1 + x^{-1/t}\right)$, and we can write

$$T(\boldsymbol{L}_t) = \boldsymbol{L}_{-1/t} + \boldsymbol{L}_0.$$

The effect T to the circulants is summarised as follows:

T	for $p \equiv 3 \pmod 8$	for $p \equiv -3 \pmod 8$
$T(\boldsymbol{R}_0)$	$\boldsymbol{R}_0 + \boldsymbol{J}$	$\boldsymbol{R}_0$
$T(\boldsymbol{R}_s)$	$\boldsymbol{R}_{-1/s} + \boldsymbol{R}_0$	$\boldsymbol{R}_{-1/s} + \boldsymbol{J}$
$T(\boldsymbol{R}_t)$	$\boldsymbol{R}_{-1/t} + \boldsymbol{R}_0 + \boldsymbol{J}$	$\boldsymbol{R}_{-1/t} + \boldsymbol{R}_0$
$T(\boldsymbol{L}_0)$	$\boldsymbol{L}_0 + \boldsymbol{J}'$	$\boldsymbol{L}_0$
$T(\boldsymbol{L}_s)$	$\boldsymbol{L}_{-1/s} + \boldsymbol{L}_0$	$\boldsymbol{L}_{-1/s} + \boldsymbol{J}'$
$T(\boldsymbol{L}_t)$	$\boldsymbol{L}_{-1/t} + \boldsymbol{L}_0 + \boldsymbol{J}'$	$\boldsymbol{L}_{-1/t} + \boldsymbol{L}_0$

where $s \in Q$ and $t \in N$. This shows that, for $p \equiv \pm 3 \pmod 8$, the transformation T is a linear combination of at most three rows of the circulant and hence it fixes the circulant. This establishes the following theorem on $\mathrm{Aut}(\mathscr{B}_p)$ [2, 13].

Theorem 9.1 *The automorphism group of the* $(2(p+1), p+1, d)$ *binary quadratic double-circulant codes contains* $PSL_2(p)$ *applied simultaneously to both circulants.*

The knowledge of $\mathrm{Aut}(\mathscr{B}_p)$ can be exploited to deduce the modular congruence weight distributions of $\mathscr{B}_p$ as shown in Sect. 9.6.

9.5 Evaluation of the Number of Codewords of Given Weight and the Minimum Distance: A More Efficient Approach

In Chap. 5 algorithms to compute the minimum distance of a binary linear code and to count the number of codewords of a given weight are described. Assuming the code rate of the code is a half and its generator matrix contains two mutually disjoint information sets, each of rank k (the code dimension), these algorithms require enumeration of

$$\binom{k}{w/2} + 2\sum_{i=1}^{w/2-1}\binom{k}{i}$$

codewords in order to count the number of codewords of weight w. For FSD double-circulant codes with $p \equiv -3 \pmod 8$ and self-dual double-circulant codes a more efficient approach exists. This approach applies to both pure and bordered double-circulant cases.

Lemma 9.7 *Let $T_m(x)$ be a set of binary polynomials with degree at most m. Let $u_i(x), v_i(x) \in T_{k-1}(x)$ for $i = 1, 2$, and $e(x), f(x) \in T_{k-2}(x)$. The numbers of weight w codewords of the form $c_1(x) = (u_1(x)|v_1(x))$ and $c_2(x) = (v_2(x)|u_2(x))$ are equal, where*

(i) for self-dual pure double-circulant codes, $u_2(x) = u_1(x)^T$ and $v_2(x) = v_1(x)^T$;
(ii) for self-dual bordered double-circulant codes, $u_1(x) = (\varepsilon|e(x))$, $v_1(x) = (\gamma|f(x))$, $u_2(x) = (\varepsilon|e(x)^T)$ and $v_2(x) = (\gamma|f(x)^T)$, where $\gamma = \mathrm{wt}_H(e(x)) \pmod 2$;
(iii) for FSD pure double-circulant codes ($p \equiv -3 \pmod 8$), $u_2(x) = u_1(x)^2$ and $v_2(x) = v_1(x)^2$;
(iv) for FSD bordered double-circulant codes ($p \equiv -3 \pmod 8$), $u_1(x)=(\varepsilon|e(x))$, $v_1(x) = (\gamma|f(x))$, $u_2(x) = (\varepsilon|e(x)^2)$, $v_2(x) = (\gamma|f(x)^2)$, where $\gamma = \mathrm{wt}_H(e(x)) \pmod 2$.

Proof

(i) Let $\boldsymbol{G}_1 = [\boldsymbol{I}_k|\boldsymbol{R}]$ and $\boldsymbol{G}_2 = [\boldsymbol{R}^T|\boldsymbol{I}_k]$ be the two full-rank generator matrices with mutually disjoint information sets of a self-dual pure double-circulant code. Assume that $r(x)$ and $r(x)^T$ are the defining polynomials of $\boldsymbol{G}_1$ and $\boldsymbol{G}_2$, respectively. Given $u_1(x)$ as an input, we have a codeword $c_1(x) = (u_1(x)|v_1(x))$, where $v_1(x) = u_1(x)r(x)$, from $\boldsymbol{G}_1$. Another codeword $c_2(x)$ can be obtained from $\boldsymbol{G}_2$ using $u_1(x)^T$ as an input, $c_2(x) = (v_1(x)^T|u_1(x)^T)$, where $v_1(x)^T = u_1(x)^T r(x)^T = (u_1(x)r(x))^T$. Since the weight of a polynomial and that of its transpose are equal, for a given polynomial of degree at most $k-1$, there exist two distinct codewords of the same weight.

(ii) Let $\boldsymbol{G}_1$, given by (9.5b), and $\boldsymbol{G}_2$ be two full-rank generator matrices with pairwise disjoint information sets, of bordered self-dual double-circulant codes. It is assumed that the form of $\boldsymbol{G}_2$ is identical to that given by (9.21) with $\boldsymbol{R}^T = \boldsymbol{B}^T$. Let $f(x) = e(x)r(x)$, consider the following cases:

a. $\varepsilon = 0$ and $\mathrm{wt}_H(e(x))$ is odd, we have a codeword $c_1(x) = (0 \mid e(x) \mid 1 \mid f(x))$ from $\boldsymbol{G}_1$. Applying $\left(0 \mid e(x)^T\right)$ as an information vector to $\boldsymbol{G}_2$, we have another codeword $c_2(x) = \left(1 \mid e(x)^T r(x)^T \mid 0 \mid e(x)^T\right) = \left(1 \mid f(x)^T \mid 0 \mid e(x)^T\right)$.

b. $\varepsilon = 1$ and $\mathrm{wt}_H(e(x))$ is odd, $\boldsymbol{G}_1$ produces $c_1(x) = (1 \mid e(x) \mid 1 \mid f(x) + j(x))$. Applying $\left(1 \mid e(x)^T\right)$ as an information vector to $\boldsymbol{G}_2$, we have a codeword $c_2(x) = \left(1 \mid e(x)^T r(x)^T + j(x) \mid 1 \mid e(x)^T\right) = \left(1 \mid f(x)^T + j(x) \mid 1 \mid e(x)^T\right)$.

c. $\varepsilon = 0$ and $\mathrm{wt}_H(e(x))$ is even, $\boldsymbol{G}_1$ produces a codeword $c_1(x) = (0 \mid e(x) \mid 0 \mid f(x))$. Applying $\left(0 \mid e(x)^T\right)$ as an information vector to $\boldsymbol{G}_2$, we have another codeword $c_2(x) = \left(0 \mid e(x)^T r(x)^T \mid 0 \mid e(x)^T\right) = \left(0 \mid f(x)^T \mid 0 \mid e(x)^T\right)$.

d. $\varepsilon = 1$ and $\mathrm{wt}_H(e(x))$ is even, $\boldsymbol{G}_1$ produces $c_1(x) = (1 \mid e(x) \mid 0 \mid f(x) + j(x))$. Applying $\left(1 \mid e(x)^T\right)$ as an information vector to $\boldsymbol{G}_2$, we have a codeword $c_2(x) = \left(0 \mid e(x)^T r(x)^T + j(x) \mid 1 \mid e(x)^T\right) = \left(0 \mid f(x)^T + j(x) \mid 1 \mid e(x)^T\right)$.

It is clear that in all cases, $\mathrm{wt}_H(c_1(x)) = \mathrm{wt}_H(c_2(x))$ since $\mathrm{wt}_H(v(x)) = \mathrm{wt}_H(v(x)^T)$ and $\mathrm{wt}_H(v(x) + j(x)) = \mathrm{wt}_H(v(x)^T + j(x))$ for some polynomial $v(x)$. This means that given an information vector, there always exist two distinct codewords of the same weight.

(iii) Let $\boldsymbol{G}_1$, given by (9.5a) with $\boldsymbol{R} = \boldsymbol{I}_p + \boldsymbol{Q}$, and $\boldsymbol{G}_2$, given by (9.18), be two full-rank generator matrices with pairwise disjoint information sets, of pure FSD double-circulant codes for $p \equiv -3 \pmod 8$.
Given $u_1(x)$ as input, we have a codeword $c_1(x) = (u_1(x)|v_1(x))$, where $v_1(x) = u_1(x)(1 + q(x))$, from $\boldsymbol{G}_1$ and another codeword $c_2(x) = (v_2(x)|u_2(x))$, where $u_2(x) = u_1(x)^2$ and $v_2(x) = u_1(x)^2(1 + n(x)) = u_1(x)^2(1 + q(x))^2 = v_1(x)^2$, from $\boldsymbol{G}_2$. Since the weight of a polynomial and that of its square are the same over $\mathbb{F}_2$, the proof follows.

(iv) Let $\boldsymbol{G}_1$, given by (9.5b) with $\boldsymbol{B} = \boldsymbol{R}$, and $\boldsymbol{G}_2$, given by (9.22), be two full-rank generator matrices with pairwise disjoint information sets, of bordered FSD double-circulant codes for $p \equiv -3 \pmod 8$. Let $f(x) = e(x)b(x)$, consider the following cases:

a. $\varepsilon = 0$ and $\mathrm{wt}_H(e(x))$ is odd, we have a codeword $c_1(x) = (0 \mid e(x) \mid 1 \mid f(x))$ from $\boldsymbol{G}_1$. Applying $\left(0 \mid e(x)^2\right)$ as an information vector to $\boldsymbol{G}_2$, we have another codeword $c_2(x) = \left(1 \mid e(x)^2 n(x) \mid 0 \mid e(x)^2\right)$. Since $e(x)^2 n(x) = e(x)^2 b(x)^2 = f(x)^2$, the codeword $c_2 = \left(1 \mid f(x)^2 \mid 0 \mid e(x)^2\right)$.
b. $\varepsilon = 1$ and $\mathrm{wt}_H(e(x))$ is odd, $\boldsymbol{G}_1$ produces $c_1(x) = (1 \mid e(x) \mid 1 \mid f(x) + j(x))$. Applying $\left(1 \mid e(x)^2\right)$ as an information vector to $\boldsymbol{G}_2$, we have a codeword $c_2(x) = \left(1 \mid e(x)^2 n(x) + j(x) \mid 1 \mid e(x)^2\right) = \left(1 \mid f(x)^2 + j(x) \mid 1 \mid e(x)^2\right)$.
c. $\varepsilon = 0$ and $\mathrm{wt}_H(e(x))$ is even, $\boldsymbol{G}_1$ produces a codeword $c_1(x) = (0 \mid e(x) \mid 0 \mid f(x))$. Applying $\left(0 \mid e(x)^2\right)$ as an information vector to $\boldsymbol{G}_2$, we have another codeword $c_2(x) = \left(0 \mid e(x)^2 n(x) \mid 0 \mid e(x)^2\right) = \left(0 \mid f(x)^2 \mid 0 \mid e(x)^2\right)$.
d. $\varepsilon = 1$ and $\mathrm{wt}_H(e(x))$ is even, $\boldsymbol{G}_1$ produces $c_1(x) = (1 \mid e(x) \mid 0 \mid f(x) + j(x))$. Applying $\left(1 \mid e(x)^2\right)$ as an information vector to $\boldsymbol{G}_2$, we have a codeword $c_2(x) = \left(0 \mid e(x)^2 n(x) + j(x) \mid 1 \mid e(x)^2\right) = \left(0 \mid f(x)^2 + j(x) \mid 1 \mid e(x)^2\right)$.

It is clear that in all cases, $\mathrm{wt}_H(c_1(x)) = \mathrm{wt}_H(c_2(x))$ since $\mathrm{wt}_H(v(x)) = \mathrm{wt}_H(v(x)^2)$ and $\mathrm{wt}_H(v(x) + j(x)) = \mathrm{wt}_H(v(x)^2 + j(x))$ for some polynomial $v(x)$. This means that given an information vector, there always exist two distinct codewords of the same weight.

From Lemma 9.7, it follows that, in order to count the number of codewords of weight w, we only require

$$\sum_{i=1}^{w/2} \binom{k}{i}$$

codewords to be enumerated and if A_w denotes the number of codewords of weight w,

$$A_w = a_{w/2} + 2 \sum_{i=1}^{w/2-1} a_i \tag{9.26}$$

where a_i is the number of weight w codewords which have i non-zeros in the first k coordinates.

Similarly, the commonly used method to compute the minimum distance of half-rate codes with two full-rank generator matrices of mutually disjoint information sets, for example, see van Dijk et al. [18], assuming that d is the minimum distance of the code, requires as many as

$$S = 2 \sum_{i=1}^{d/2-1} \binom{n}{i}$$

codewords to be enumerated. Following Lemma 9.7, only $S/2$ codewords are required for $\mathscr{P}_p$ and $\mathscr{B}_p$ for $p \equiv -3 \pmod 8$, and self-dual double-circulant codes. Note that the bound $d/2 - 1$ may be improved for singly even and doubly even codes, but we consider the general case here.

9.6 Weight Distributions

The automorphism group of both $(p+1, \frac{1}{2}(p+1), d)$ extended QR and $(2(p+1), p+1, d)$ quadratic double-circulant codes contains the projective special linear group, $\mathrm{PSL}_2(p)$. Let $\mathscr{H}$ be a subgroup of the automorphism group of a linear code, and the number of codewords of weight i, denoted by A_i, can be categorised into two classes:

1. a class of weight i codewords which are invariant under some element of $\mathscr{H}$; and
2. a class of weight i codewords which forms an orbit of size $|\mathscr{H}|$, the order of $\mathscr{H}$. In the other words, if $\boldsymbol{c}$ is a codeword of this class, applying all elements of $\mathscr{H}$ to $\boldsymbol{c}$, $|\mathscr{H}|$ distinct codewords are obtained.

Thus, we can write A_i in terms of congruence as follows:

$$\begin{aligned} A_i &= n_i \times |\mathscr{H}| + A_i(\mathscr{H}), \\ &\equiv A_i(\mathscr{H}) \pmod{|\mathscr{H}|} \end{aligned} \tag{9.27}$$

where $A_i(\mathscr{H})$ is the number of codewords of weight i fixed by some element of $\mathscr{H}$. This was originally shown by Mykkeltveit et al. [14], where it was applied to extended QR codes for primes 97 and 103.

9.6.1 The Number of Codewords of a Given Weight in Quadratic Double-Circulant Codes

For $\mathscr{B}_p$, we shall choose $\mathscr{H} = \mathrm{PSL}_2(p)$, which has order $|\mathscr{H}| = \frac{1}{2}p(p^2-1)$. Let the matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ represent an element of $\mathrm{PSL}_2(p)$, see (9.23). Since $|\mathscr{H}|$ can be factorised as $|\mathscr{H}| = \prod_j q_j^{e_j}$, where q_j is a prime and e_j is some integer, $A_i(\mathscr{H})$ (mod $|\mathscr{H}|$) can be obtained by applying the Chinese remainder theorem to $A_i(S_{q_j})$ (mod $q_j^{e_j}$) for all q_j that divides $|\mathscr{H}|$, where S_{q_j} is the Sylow-q_j-subgroup of $\mathscr{H}$. In order to compute $A_i(S_{q_j})$, a subcode of $\mathscr{B}_p$ which is invariant under S_{q_j} needs to be obtained in the first place. This invariant subcode, in general, has a considerably smaller dimension than $\mathscr{B}_p$, and hence, its weight distribution can be easily obtained.

For each odd prime q_j, S_{q_j} is a cyclic group which can be generated by some $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{PSL}_2(p)$ of order q_j. Because S_{q_j} is cyclic, it is straightforward to obtain the invariant subcode, from which we can compute $A_i(S_{q_j})$.

On the other hand, the case of $q_j = 2$ is more complicated. For $q_j = 2$, S_2 is a dihedral group of order 2^{m+1}, where $m+1$ is the maximum power of 2 that divides $|\mathscr{H}|$ [**?**]. For $p = 8m \pm 3$, we know that

$$|\mathscr{H}| = \frac{1}{2}(8m \pm 3)\left((8m \pm 3)^2 - 1\right) = 2^2\left(64m^3 \pm 72m^2 + 26m \pm 3\right),$$

which shows that the highest power of 2 that divides $|\mathscr{H}|$ is 2^2 ($m = 1$). Following [**?**], there are $2^m + 1$ subgroups of order 2 in S_2, namely

$$\begin{aligned} H_2 &= \{1, P\}, \\ G_2^0 &= \{1, T\}, \text{ and} \\ G_2^1 &= \{1, PT\}, \end{aligned}$$

where $P, T \in \mathrm{PSL}_2(p)$, $P^2 = T^2 = 1$ and $TPT^{-1} = P^{-1}$.

Let $T = \left[\begin{smallmatrix} 0 & p-1 \\ 1 & 0 \end{smallmatrix}\right]$, which has order 2. It can be shown that any order 2 permutation, $P = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, if a constraint $b = c$ is imposed, we have $a = -d$. All these subgroups, however, are conjugates in $\mathrm{PSL}_2(p)$ [**?**] and therefore, the subcodes fixed by G_2^0, G_2^1 and H_2 have identical weight distributions and considering any of them, say G_2^0, is sufficient.

Apart from $2^m + 1$ subgroups of order 2, S_2 also contains a cyclic subgroup of order 4, 2^{m-1} non-cyclic subgroups of order 4, and subgroups of order 2^j for $j \geq 3$.

Following [14], only the subgroups of order 2 and the non-cyclic subgroups of order 4 make contributions towards $A_i(S_2)$. For $p \equiv \pm 3 \pmod 8$, there is only one non-cyclic subgroup of order 4, denoted by G_4, which contains, apart from an identity, three permutations of order 2 [**?**], i.e. a Klein 4 group,

$$G_4 = \{1, P, T, PT\}.$$

Having obtained $A_i(G_2^0)$ and $A_i(G_4)$, following the argument in [14], the number of codewords of weight i that are fixed by some element of S_2 is given by

$$A_i(S_2) \equiv 3A_i(G_2^0) - 2A_i(G_4) \pmod 4. \tag{9.28}$$

In summary, in order to deduce the modular congruence of the number of weight i codewords in $\mathscr{B}_p$, it is sufficient to do the following steps:

1. compute the number of weight i codewords in the subcodes fixed by G_2^0, G_4 and S_q, for all odd primes q that divide $|\mathscr{H}|$;
2. apply (9.28) to $A_i(G_2^0)$ and $A_i(G_4)$ to obtain $A_i(S_2)$; and then
3. apply the Chinese remainder theorem to $A_i(S_2)$ and all $A_i(S_q)$ to obtain $A_i(\mathscr{H}) \pmod{|\mathscr{H}|}$.

Given $\mathscr{B}_p$ and an element of $\mathrm{PSL}_2(p)$, how can we find the subcode consisting of the codewords fixed by this element? Assume that $Z = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{PSL}_2(p)$ of prime order. Let c_{l_i} (resp. c_{r_i}) and $c_{l_{i'}}$ (resp. $c_{r_{i'}}$) denote the ith coordinate and $\pi_Z(i)$th coordinate (ith coordinate with the respect to permutation π_Z), in the left (resp. right) circulant form, respectively. The invariant subcode can be obtained by solving a set of linear equations consisting of the parity-check matrix of $\mathscr{B}_p$ (denoted by $\boldsymbol{H}$), $c_{l_i} + c_{l_{i'}} = 0$ (denoted by $\boldsymbol{\pi}_Z(L)$) and $c_{r_i} + c_{r_{i'}} = 0$ (denoted by $\boldsymbol{\pi}_Z(R)$) for all $i \in \mathbb{F}_p \cup \{\infty\}$, i.e.

$$\boldsymbol{H}_{sub} = \begin{array}{|c|}\hline \boldsymbol{H} \\ \hline \boldsymbol{\pi}_Z(L) \\ \hline \boldsymbol{\pi}_Z(R) \\ \hline \end{array}.$$

The solution to $\boldsymbol{H}_{sub}$ is a matrix of rank $r > (p+1)$, which is the parity-check matrix of the $(2(p+1), 2(p+1) - r, d')$ invariant subcode. For subgroup G_4, which consists of permutations P, T and PT, we need to solve the following matrix

$$\boldsymbol{H}_{sub} = \begin{array}{|c|}\hline \boldsymbol{H} \\ \hline \boldsymbol{\pi}_P(L) \\ \hline \boldsymbol{\pi}_P(R) \\ \hline \boldsymbol{\pi}_T(L) \\ \hline \boldsymbol{\pi}_T(R) \\ \hline \boldsymbol{\pi}_{PT}(L) \\ \hline \boldsymbol{\pi}_{PT}(R) \\ \hline \end{array}$$

to obtain the invariant subcode. Note that the parity-check matrix of $\mathscr{B}_p$ is assumed to have the following form:

$$\boldsymbol{H} = \begin{array}{c|ccc|c|ccc} l_\infty & l_0 & \dots & l_{p-1} & r_\infty & r_0 & \dots & r_{p-1} \\ \hline 0 & & & & 1 & & & \\ \vdots & & \boldsymbol{B}^T & & \vdots & & \boldsymbol{I}_p & \\ 0 & & & & 1 & & & \\ \hline 1 & 1 & \dots & 1 & 0 & 0 & \dots & 0 \end{array}. \tag{9.29}$$

One useful application of the modular congruence of the number of codewords of weight w is to verify, independently, the number of codewords of a given weight w that were computed exhaustively.

Computing the number of codewords of a given weight in small codes using a single-threaded algorithm is tractable, but for longer codes, it is necessary to use multiple computers working in parallel to produce a result within a reasonable time. Even so it can take several weeks, using hundreds of computers, to evaluate a long code. In order to do the splitting, the codeword enumeration task is distributed among all of the computers and each computer just needs to evaluate a predetermined number of codewords, finding the partial weight distributions. In the end, the results are combined to give the total number of codewords of a given weight. There is always the possibility of software bugs or mistakes to be made, particularly in any parallel computing scheme. The splitting may not be done correctly or double-counting or miscounting introduced as a result, apart from possible errors in combining the partial results. Fortunately, the modular congruence approach can also provide detection of computing errors by revealing inconsistencies in the summed results. The importance of this facet of modular congruence will be demonstrated in determining the weight distributions of extended QR codes in Sect. 9.6.2. In the following examples we work through the application of the modular congruence technique in evaluating the weight distributions of the quadratic double-circulant codes of primes 37 and 83.

Example 9.1 For prime 37, there exists an FSD $(76, 38, 12)$ quadratic double-circulant code, $\mathscr{B}_{37}$. The weight enumerator of an FSD code is given by Gleason's theorem [15]

$$A(z) = \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} K_i (1 + z^2)^{\frac{n}{2}-4i} (z^2 - 2z^4 + z^6)^i \tag{9.30}$$

for integers K_i. The number of codewords of any weight w is given by the coefficient of z^w of $A(z)$. In order to compute $A(z)$ of $\mathscr{B}_{37}$, we need only to compute A_{2i} for $6 \leq i \leq 9$. Using the technique described in Sect. 9.5, the number of codewords of desired weights is obtained and then substituted into (9.30). The resulting weight enumerator function giving the whole weight distribution of the $(76, 38, 12)$ code, $\mathscr{B}_{37}$ is

$$\begin{aligned} A(z) = &\left(1 + z^{76}\right) + 2109 \times \left(z^{12} + z^{64}\right) + \\ &86469 \times \left(z^{16} + z^{60}\right) + 961704 \times \left(z^{18} + z^{58}\right) + \\ &7489059 \times \left(z^{20} + z^{56}\right) + 53574224 \times \left(z^{22} + z^{54}\right) + \\ &275509215 \times \left(z^{24} + z^{52}\right) + 1113906312 \times \left(z^{26} + z^{50}\right) + \\ &3626095793 \times \left(z^{28} + z^{48}\right) + 9404812736 \times \left(z^{30} + z^{46}\right) + \\ &19610283420 \times \left(z^{32} + z^{44}\right) + 33067534032 \times \left(z^{34} + z^{42}\right) + \\ &45200010670 \times \left(z^{36} + z^{40}\right) + 50157375456 \times z^{38}. \end{aligned} \tag{9.31}$$

Let $\mathscr{H} = \mathrm{PSL}_2(37)$, and we know that $|\mathscr{H}| = 2^2 \times 3^2 \times 19 \times 37 = 25308$. Consider the odd primes as factors q. For $q = 3$, $\left[\begin{smallmatrix} 0 & 1 \\ 36 & 1 \end{smallmatrix}\right]$ generates the following permutation of order 3:

$$(\infty, 0, 1)(2, 36, 19)(3, 18, 13)(4, 12, 10)(5, 9, 23)(6, 22, 7)(8, 21, 24)$$
$$(11)(14, 17, 30)(15, 29, 33)(16, 32, 31)(20, 35, 25)(26, 34, 28)(27)$$

The corresponding invariant subcode has a generator matrix $G^{(S_3)}$ of dimension 14, which is given by

$$\boldsymbol{G}^{(S_3)} = \begin{bmatrix}
1000000000000011101110011111101001001011001010001001110001000100000000000000 \\
0100000000000000001001100010111011000100010111001101110000001000000000100000 \\
0010000000000011101011101010110011010110101001000011110100000001000000000000 \\
0001000000000011100111111111000100001111010100110101110010000010000000000000 \\
0000100000000011101011111010101001011111111110001111110000000000000000000000 \\
0000010000000011111111111111111111111111111111111111110000000000000000000000 \\
0000001000000011101110001111111111010010101011111011110000000000000000000000 \\
0000000100000000000110011101000100011011101000110011110000000000100100000000 \\
0000000010000011101101100101110111000100011101110101110000110000000000000000 \\
0000000001000011100101110111000100011101110100110111110000000000001000000001 \\
0000000000100011100010001010011010010010111111001111110000000000010000000010 \\
0000000000010011100101100101011110000100011111111101110000000000000000001100 \\
0000000000001011101000010010101101011001101010111011110000000000000001010000 \\
0000000000000100001111101111101101010110111110111111111000000000000010000000
\end{bmatrix}$$

and its weight enumerator function is

$$\begin{aligned} A^{(S_3)}(z) = &\left(1 + z^{76}\right) + 3 \times \left(z^{12} + z^{64}\right) + 24 \times \left(z^{16} + z^{60}\right) + \\ &54 \times \left(z^{18} + z^{58}\right) + 150 \times \left(z^{20} + z^{56}\right) + 176 \times \left(z^{22} + z^{54}\right) + \\ &171 \times \left(z^{24} + z^{52}\right) + 468 \times \left(z^{26} + z^{50}\right) + 788 \times \left(z^{28} + z^{48}\right) + \\ &980 \times \left(z^{30} + z^{46}\right) + 1386 \times \left(z^{32} + z^{44}\right) + 1350 \times \left(z^{34} + z^{42}\right) + \\ &1573 \times \left(z^{36} + z^{40}\right) + 2136 \times z^{38}. \end{aligned} \tag{9.32}$$

For $q = 19$, $\left[\begin{smallmatrix} 0 & 1 \\ 36 & 3 \end{smallmatrix}\right]$ generates the following permutation of order 19:

$$(\infty, 0, 25, 5, 18, 32, 14, 10, 21, 2, 1, 19, 30, 26, 8, 22, 35, 15, 3)$$
$$(4, 36, 28, 34, 31, 33, 16, 17, 29, 27, 20, 13, 11, 23, 24, 7, 9, 6, 12).$$

The resulting generator matrix of the invariant subcode $\boldsymbol{G}^{(S_{19})}$, which has dimension 2, is

$$G^{(S_{19})} = \begin{bmatrix} 1011111111111111111111111111111111111110000000000000000000000000000000000000 \\ 0100000000000000000000000000000000000001111111111111111111111111111111111111 \end{bmatrix}$$

and its weight enumerator function is

$$A^{(S_{19})}(z) = 1 + 2z^{38} + z^{76}. \tag{9.33}$$

For the last odd prime, $q = 37$, a permutation of order 37

$$(\infty, 0, 18, 24, 27, 14, 30, 15, 13, 32, 25, 26, 33, 19, 7, 4, 6, 23, 34,$$
$$1, 12, 29, 31, 28, 16, 2, 9, 10, 3, 22, 20, 5, 21, 8, 11, 17, 35)(36)$$

is generated by $\left[\begin{smallmatrix} 0 & 1 \\ 36 & 35 \end{smallmatrix}\right]$ and it turns out that the corresponding invariant subcode, and hence, the weight enumerator function, are identical to those of $q = 19$.

For $q = 2$, subcodes fixed by some element of G_2^0 and G_4 are required. We have $P = \left[\begin{smallmatrix} 3 & 8 \\ 8 & 34 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 36 \\ 1 & 0 \end{smallmatrix}\right]$, and the resulting order 2 permutations generated by P, T and PT are

$$(\infty, 5)(0, 22)(1, 17)(2, 21)(3, 29)(4, 16)(6, 31)(7, 18)(8, 26)(9, 30)(10, 25)$$
$$(11, 34)(12, 14)(13, 36)(15)(19, 28)(20, 24)(23, 27)(32)(33, 35)$$

$$(\infty, 0)(1, 36)(2, 18)(3, 12)(4, 9)(5, 22)(6)(7, 21)(8, 23)(10, 11)(13, 17)$$
$$(14, 29)(15, 32)(16, 30)(19, 35)(20, 24)(25, 34)(26, 27)(28, 33)(31)$$

and

$$(\infty, 22)(0, 5)(1, 13)(2, 7)(3, 14)(4, 30)(6, 31)(8, 27)(9, 16)(10, 34)(11, 25)$$
$$(12, 29)(15, 32)(17, 36)(18, 21)(19, 33)(20)(23, 26)(24)(28, 35)$$

respectively. It follows that the corresponding generator matrices and weight enumerator functions of the invariant subcodes are

$$G^{(G_2^0)} = \begin{bmatrix}
1000000000000000000001010101100011010101011101000000010111001000000000000000 \\
0100000000000000000010111000011000011000011101010110110100000000100000000000 \\
0010000000000000000010110111011001011110001000010001111011000000000000000000 \\
0001000000000000000001100100111101010111100100110101001010000000000001000000 \\
0000100000000000000010000110111011011101100000001010101010000100000000000000 \\
0000010000000000000010110010010111010010011001110000001110100000000000000000 \\
0000001000000000000011111111111111111111111111111111111110000000000000000000 \\
0000000100000000000000001100001111011100100000100111011110000000000000000100 \\
0000000010000000000000101101100110001111110001100110110100000000001000000000 \\
0000000001000000000001000100111111010101010111111001000100000000010000000000 \\
0000000000100000000010011110011110000100011011111011000100000000000000000010 \\
0000000000010000000011100000011100000101001111111100101000000000000000001000 \\
0000000000001000000011000011101010110110101011100001100000000100000000000000 \\
0000000000000100000011110010101010001011111110100010101010000000010000000000 \\
0000000000000010000011001011010111011000000110111010110100000001000000000000 \\
0000000000000001000000001100011000101100111101101111001101000000000000010000 \\
0000000000000000100000101001011011010010100010011111100100000010000000000000 \\
0000000000000000010011101110110000000011110011001111000000000000000010000000 \\
0000000000000000001001111001001101010010101100100111101010000000000000000001 \\
0000000000000000000110011011101100000001111001100111100000000000000000100000
\end{bmatrix},$$

which has dimension 20, with

$$A^{(G_2^0)}(z) = \left(1 + z^{76}\right) + 21 \times \left(z^{12} + z^{64}\right) + 153 \times \left(z^{16} + z^{60}\right) + \\ 744 \times \left(z^{18} + z^{58}\right) + 1883 \times \left(z^{20} + z^{56}\right) + 4472 \times \left(z^{22} + z^{54}\right) + \\ 10119 \times \left(z^{24} + z^{52}\right) + 21000 \times \left(z^{26} + z^{50}\right) + 36885 \times \left(z^{28} + z^{48}\right) + \\ 58656 \times \left(z^{30} + z^{46}\right) + 85548 \times \left(z^{32} + z^{44}\right) + 108816 \times \left(z^{34} + z^{42}\right) + \\ 127534 \times \left(z^{36} + z^{40}\right) + 136912 \times z^{38} \tag{9.34}$$

and

$$\boldsymbol{G}^{(G_4)} = \begin{bmatrix} 1000000000001101101011011101000110111011111000111000100001000000000010000000 \\ 0100000000000000010100111000110001000110000111010110000100000000000000000000 \\ 0010000000001101101010000101000100110000001000000000000000100000000000010100 \\ 0001000000001111111111111111111111111111111111111000000000000000000000000000 \\ 0000100000000000010100100000110011000100010111101000010000000010100000000000 \\ 0000010000001101101111000101100101111101101011000000001000010000001000000000 \\ 0000001000001100101101011101100000011011101011010000000010000000000000000000 \\ 0000000100000001100011000101100111101101111001101000000000000000100000000000 \\ 0000000010000000110000111101110010000010011101111000000000000000000000100000 \\ 0000000001001100001101011000100001011111100011010000000000001100000000001000 \\ 0000000000100000100101000101100011001101111011101000000000000000000001000011 \\ 0000000000011100111000111101010010010010011100111001000000000001000100000000 \end{bmatrix},$$

which has dimension 12, with

$$A^{(G_4)}(z) = \left(1 + z^{76}\right) + 3 \times \left(z^{12} + z^{64}\right) + 11 \times \left(z^{16} + z^{60}\right) + \\ 20 \times \left(z^{18} + z^{58}\right) + 51 \times \left(z^{20} + z^{56}\right) + 56 \times \left(z^{22} + z^{54}\right) + \\ 111 \times \left(z^{24} + z^{52}\right) + 164 \times \left(z^{26} + z^{50}\right) + 187 \times \left(z^{28} + z^{48}\right) + \\ 224 \times \left(z^{30} + z^{46}\right) + 294 \times \left(z^{32} + z^{44}\right) + 328 \times \left(z^{34} + z^{42}\right) + \\ 366 \times \left(z^{36} + z^{40}\right) + 464 \times z^{38} \tag{9.35}$$

respectively. Consider the number of codewords of weight 12, from (9.31)–(9.35), we know that $A_{12}(G_2^0) = 21$ and $A_{12}(G_4) = 3$; applying (9.28),

$$A_{12}(S_2) \equiv 3 \times 21 - 2 \times 3 \pmod 4 \equiv 1 \pmod 4$$

and thus, we have the following set of simultaneous congruences:

$$\begin{aligned} A_{12}(S_2) &\equiv 1 \pmod{2^2} \\ A_{12}(S_3) &\equiv 3 \pmod{3^2} \\ A_{12}(S_{19}) &\equiv 0 \pmod{19} \\ A_{12}(S_{37}) &\equiv 0 \pmod{37}. \end{aligned}$$

Following the Chinese remainder theorem, a solution to the above congruences, denoted by $A_{12}(\mathscr{H})$, is congruent modulo LCM$\{2^2, 3^2, 19, 37\}$, where LCM$\{2^2, 3^2, 19, 37\}$ is the least common multiple of the moduli 2^2, 3^2, 19 and 37, which is equal to $2^2 \times 3^2 \times 19 \times 37 = 25308$ in this case. Since these moduli are pairwise coprime, by the extended Euclidean algorithm, we can write

$$1 = 4 \times 1582 + \frac{25308}{4} \times (-1)$$
$$1 = 9 \times 625 + \frac{25308}{9} \times (-2)$$
$$1 = 19 \times 631 + \frac{25308}{19} \times (-9)$$
$$1 = 37 \times 37 + \frac{25308}{37} \times (-2).$$

A solution to the congruences above is given by

$$\begin{aligned} A_{12}(\mathscr{H}) &= 1 \times \left[(-1)\frac{25308}{4}\right] + 3 \times \left[(-2)\frac{25308}{9}\right] + 0 \times \left[(-9)\frac{25308}{19}\right] \\ &\quad + 0 \times \left[(-2)\frac{25308}{37}\right] \pmod{25308} \\ &= -1 \times 6327 + -6 \times 2812 \pmod{25308} \\ &= 2109 \pmod{25308} \\ &= 25308 n_{12} + 2109. \end{aligned}$$

Referring to the weight enumerator function, (9.31), we can immediately see that $n_{12} = 0$, indicating that A_{12} has been accurately evaluated. Repeating the above procedures for weights larger than 12, we have Table 9.3 which shows that the weight distributions of $\mathscr{B}_{37}$ are indeed accurate. In fact, since the complete weight distrib-

Table 9.3 Modular congruence weight distributions of $\mathscr{B}_{37}$

$i/n-i$	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3^2	$A_i(S_{19})$ mod 19	$A_i(S_{37})$ mod 37	$A_i(\mathscr{H})$ mod 25308	n_i in $A_i = 25308n_i + A_i(\mathscr{H})$
0/76	1	1	1	1	1	0
12/64	1	3	0	0	2109	0
16/60	1	6	0	0	10545	3
18/58	0	0	0	0	0	38
20/56	3	6	0	0	23199	295
22/54	0	5	0	0	22496	2116
24/52	3	0	0	0	6327	10886
26/50	0	0	0	0	0	44014
28/48	1	5	0	0	16169	143278
30/46	0	8	0	0	5624	371614
32/44	0	0	0	0	0	774865
34/42	0	0	0	0	0	1306604
36/40	2	7	0	0	23902	1785996
38	0	3	2	2	7032	1981878

utions can be obtained once the first few terms required by Gleason's theorem are known, verification of these few terms is sufficient.

Example 9.2 Gulliver et al. [6] have shown that the (168, 84, 24) doubly even self-dual quadratic double-circulant code $\mathscr{B}_{83}$ is not extremal since it has minimum distance less than or equal to 28. The weight enumerator of a Type-II code of length n is given by Gleason's theorem, which is expressed as [15]

$$A(z) = \sum_{i=0}^{\lfloor n/24 \rfloor} K_i (1 + 14z^4 + z^8)^{\frac{n}{8}-3i} \{z^4(1-z^4)^4\}^i, \tag{9.36}$$

where K_i are some integers. As shown by (9.36), only the first few terms of A_i are required in order to completely determine the weight distribution of a Type-II code. For $\mathscr{B}_{83}$, only the first eight terms of A_i are required. Using the parallel version of the efficient codeword enumeration method described in Chap. 5, Sect. 9.5, we determined that all of these eight terms are 0 apart from $A_0 = 1$, $A_{24} = 571704$ and $A_{28} = 17008194$.

We need to verify independently whether or not A_{24} and A_{28} have been correctly evaluated. As in the previous example, the modular congruence method can be used for this purpose. For $p = 83$, we have $|\mathscr{H}| = 2^2 \times 3 \times 7 \times 41 \times 83 = 285852$. We will consider the odd prime cases in the first place.

For prime $q = 3$, a cyclic group of order 3, S_3 can be generated by $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 1 \end{smallmatrix}\right] \in \mathrm{PSL}_2(83)$, and we found that the subcode invariant under S_3 has dimension 28 and has 63 and 0 codewords of weights 24 and 28, respectively.

For prime $q = 7$, we have $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 10 \end{smallmatrix}\right]$ which generates S_7. The subcode fixed by S_7 has dimension 12 and no codewords of weight 24 or 28 are contained in this subcode.

Similarly, for prime $q = 41$, the subcode fixed by S_{41}, which is generated by $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 4 \end{smallmatrix}\right]$ and has dimension 4, contains no codewords of weight 24 or 28.

Finally, for prime $q = 83$, the invariant subcode of dimension 2 contains the all-zeros, the all-ones, $\{\underbrace{0, 0, \ldots, 0, 0}_{84}, \underbrace{1, 1, \ldots, 1, 1}_{84}\}$ and $\{\underbrace{1, 1, \ldots, 1, 1}_{84}, \underbrace{0, 0, \ldots, 0, 0}_{84}\}$ codewords only. The cyclic group S_{83} is generated by $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 81 \end{smallmatrix}\right]$.

For the case of $q = 2$, we have $P = \left[\begin{smallmatrix} 1 & 9 \\ 9 & 82 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 82 \\ 1 & 0 \end{smallmatrix}\right]$. The subcode fixed by S_2, which has dimension 42, contains 196 and 1050 codewords of weights 24 and 28, respectively. Meanwhile, the subcode fixed by G_4, which has dimension 22, contains 4 and 6 codewords of weights 24 and 28, respectively.

Thus, using (9.28), the numbers of codewords of weights 24 and 28 fixed by S_2 are

$$A_{24}(S_2) = 3 \times 196 - 2 \times 4 \equiv 0 \pmod 4, \text{ and}$$
$$A_{28}(S_2) = 3 \times 1050 - 2 \times 6 \equiv 2 \pmod 4$$

and by applying the Chinese remainder theorem to all $A_i(S_q)$ for $i = 24, 28$, we arrive at

$$A_{24} = n_{24} \times 285852 \tag{9.37a}$$

and

$$A_{28} = n_{28} \times 285852 + 142926\,. \tag{9.37b}$$

From (9.37) we have now verified A_{24} and A_{28}, since they have equality for non-negative integers n_{24} and n_{28} ($n_{24} = 2$ and $n_{28} = 59$). Using Gleason's theorem, i.e. (9.36), the weight enumerator function of the (168, 84, 24) code $\mathscr{B}_{83}$ is obtained and it is given by

$$\begin{aligned} A(z) = {} & (z^0 + z^{168}) + \\ & 571704 \times (z^{24} + z^{144}) + \\ & 17008194 \times (z^{28} + z^{140}) + \\ & 5507510484 \times (z^{32} + z^{136}) + \\ & 1252615755636 \times (z^{36} + z^{132}) + \\ & 166058829151929 \times (z^{40} + z^{128}) + \\ & 13047194638256310 \times (z^{44} + z^{124}) + \\ & 629048483051034984 \times (z^{48} + z^{120}) + \\ & 19087129808556586056 \times (z^{52} + z^{116}) + \\ & 372099697089030108600 \times (z^{56} + z^{112}) + \\ & 4739291490433882602066 \times (z^{60} + z^{108}) + \\ & 3997367342611736981 4414 \times (z^{64} + z^{104}) + \\ & 2256966775177895002070 52 \times (z^{68} + z^{100}) + \\ & 8602411093210002174910 44 \times (z^{72} + z^{96}) + \\ & 2227390682939806465038006 \times (z^{76} + z^{92}) + \\ & 3935099587279668544910376 \times (z^{80} + z^{88}) + \\ & 4755747411704650343205104 \times z^{84}\,. \end{aligned} \tag{9.38}$$

For the complete weight distributions and their congruences of the $(2(p+1), p+1, d)$ quadratic double-circulant codes, for $11 \le p \le 83$, except $p = 37$ as it has already been given in Example 9.1, refer to Appendix "Weight Distributions of Quadratic Double-Circulant Codes and their Modulo Congruence".

9.6.2 The Number of Codewords of a Given Weight in Extended Quadratic Residue Codes

We have modified the modular congruence approach of Mykkeltveit et al. [14], which was originally introduced for extended QR codes $\hat{\mathscr{L}}_p$, so that it is applicable to the quadratic double-circulant codes. Whilst $\mathscr{B}_p$ contains one non-cyclic subgroup of order 4, $\hat{\mathscr{L}}_p$ contains two distinct non-cyclic subgroups of this order, namely G_4^0 and G_4^1. As a consequence, (9.28) becomes

$$A_i(S_2) \equiv (2^m + 1)A_i(H_2) - 2^{m-1}A_i(G_4^0) - 2^{m-1}A_i(G_4^1) \pmod{2^{m+1}}, \quad (9.39)$$

where 2^{m+1} is the highest power of 2 that divides $|\mathscr{H}|$. Unlike $\mathscr{B}_p$, where there are two circulants in which each one is fixed by $\mathrm{PSL}_2(p)$, a linear group $\mathrm{PSL}_2(p)$ acts on the entire coordinates of $\hat{\mathscr{L}}_p$. In order to obtain the invariant subcode, we only need a set of linear equations containing the parity-check matrix of $\hat{\mathscr{L}}_p$, which is arranged in $(0, 1, \ldots, p-2, p-1)(\infty)$ order, and $c_i + c_{i'} = 0$ for all $i \in \mathbb{F}_p \cup \{\infty\}$. Note that c_i and $c_{i'}$ are defined in the same manner as in Sect. 9.6.1.

We demonstrate the importance of this modular congruence approach by proving that the published results for the weight distributions of $\hat{\mathscr{L}}_{151}$ and $\hat{\mathscr{L}}_{137}$ are incorrect. However, first let us derive the weight distribution of $\hat{\mathscr{L}}_{167}$.

Example 9.3 There exists an extended QR code $\hat{\mathscr{L}}_{167}$ which has identical parameters ($n = 168$, $k = 84$ and $d = 24$) as the code $\mathscr{B}_{83}$. Since $\hat{\mathscr{L}}_{167}$ can be put into double-circulant form and it is Type-II self-dual, the algorithm in Sect. 9.5 can be used to compute the number of codewords of weights 24 and 28, denoted by A'_{24} and A'_{28} for convenience, from which we can use Gleason's theorem (9.36) to derive the weight enumerator function of the code, $A'(z)$. By codeword enumeration using multiple computers we found that

$$\begin{aligned} A'_{24} &= 776216 \\ A'_{28} &= 18130188. \end{aligned} \quad (9.40)$$

In order to verify the accuracy of A'_{24} and A'_{28}, the modular congruence method is used. In this case, we have $\mathrm{Aut}(\hat{\mathscr{L}}_{167}) \supseteq \mathscr{H} = \mathrm{PSL}_2(167)$. We also know that $|\mathrm{PSL}_2(167)| = 2^3 \times 3 \times 7 \times 83 \times 167 = 2328648$. Let $P = \left[\begin{smallmatrix} 12 & 32 \\ 32 & 155 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 166 \\ 1 & 0 \end{smallmatrix}\right]$.

Let the permutations of orders 3, 7, 83 and 167 be generated by $\left[\begin{smallmatrix} 0 & 1 \\ 166 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 166 & 19 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 166 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 166 & 165 \end{smallmatrix}\right]$, respectively. The numbers of codewords of weights 24 and 28 in the various invariant subcodes of dimension k are

	H_2	G_4^0	G_4^1	S_3	S_7	S_{83}	S_{167}
k	42	22	21	28	12	2	1
A_{24}	252	6	4	140	0	0	0
A_{28}	1812	36	0	0	6	0	0

For $\hat{\mathscr{L}}_{167}$, equation (9.39) becomes

$$A_i(S_2) \equiv 5 \times A_i(H_2) - 2 \times A_i(G_4^0) - 2 \times A_i(G_4^1) \pmod 8 . \tag{9.41}$$

It follows that

$$\begin{aligned} A_{24}(S_2) &\equiv 0 \pmod 8 \\ A_{28}(S_2) &\equiv 4 \pmod 8 \end{aligned}$$

and thus,

$$A'_{24} = n'_{24} \times 2328648 + 776216 \tag{9.42a}$$

and

$$A'_{28} = n'_{28} \times 2328648 + 1829652 \tag{9.42b}$$

from the Chinese remainder theorem.

From (9.37a) and (9.42a), we can see that $\mathscr{B}_{83}$ and $\hat{\mathscr{L}}_{167}$ are indeed inequivalent. This is because for integers $n_{24}, n'_{24} \geq 0$, $A_{24} \neq A'_{24}$.

Comparing Eq. (9.40) with (9.42a) and (9.42b) establishes that $A'_{24} = 776216$ ($n'_{24} = 0$) and $A'_{28} = 18130188$ ($n'_{28} = 7$). The weight enumerator of $\hat{\mathscr{L}}_{167}$ is derived from (9.36) and it is given in (9.43). In comparison to (9.38), it may be seen that $\hat{\mathscr{L}}_{167}$ is a slightly inferior code than $\mathscr{B}_{83}$ having more codewords of weights 24, 28 and 32.

$$\begin{aligned} A'(z) = &(z^0 + z^{168}) + \\ &776216 \times (z^{24} + z^{144}) + \\ &18130188 \times (z^{28} + z^{140}) + \\ &5550332508 \times (z^{32} + z^{136}) + \\ &1251282702264 \times (z^{36} + z^{132}) + \\ &166071600559137 \times (z^{40} + z^{128}) + \\ &13047136918828740 \times (z^{44} + z^{124}) + \\ &629048543890724216 \times (z^{48} + z^{120}) + \\ &19087130695796615088 \times (z^{52} + z^{116}) + \\ &372099690249351071112 \times (z^{56} + z^{112}) + \\ &4739291519495550245228 \times (z^{60} + z^{108}) + \\ &3997367337590380474086 \times (z^{64} + z^{104}) + \\ &2256966777271886905701 84 \times (z^{68} + z^{100}) + \end{aligned}$$

$$
\begin{aligned}
&860241108921860741947676 \times (z^{72} + z^{96}) + \\
&222739068356549178012742 8 \times (z^{76} + z^{92}) + \\
&393509958646359417246064 8 \times (z^{80} + z^{88}) + \\
&475574741259571534416937 6 \times z^{84} .
\end{aligned} \tag{9.43}
$$

Example 9.4 Gaborit et al. [4] gave A_{2i}, for $22 \leq 2i \leq 32$, of $\hat{\mathscr{L}}_{137}$ and we will check the consistency of the published results. For $p = 137$, we have $|\mathrm{PSL}_2(137)| = 2^3 \times 3 \times 17 \times 23 \times 137 = 1285608$ and we need to compute $A_{2i}(S_q)$, where $22 \leq 2i \leq 32$, for all primes q dividing $|\mathrm{PSL}_2(137)|$. Let $P = \left[\begin{smallmatrix} 137 & 51 \\ 51 & 1 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 136 \\ 1 & 0 \end{smallmatrix}\right]$.

Let $\left[\begin{smallmatrix} 0 & 1 \\ 136 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 136 & 6 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 136 & 11 \end{smallmatrix}\right]$ be generators of permutation of orders 3, 17 and 23, respectively. It is not necessary to find a generator of permutation of order 137 as it fixes the all-zeros and all-ones codewords only. Subcodes that are invariant under G_2^0, G_4^0, G_4^1, S_3, S_{17} and S_{23} are obtained and the number of weight i, for $22 \leq 2i \leq 32$, codewords in these subcodes is then computed. The results are shown as follows, where k denotes the dimension of the corresponding subcode,

	H_2	G_4^0	G_4^1	S_3	S_{17}	S_{23}	S_{137}
k	35	19	18	23	5	3	1
A_{22}	170	6	6	0	0	0	0
A_{24}	612	10	18	46	0	0	0
A_{26}	1666	36	6	0	0	0	0
A_{28}	8194	36	60	0	0	0	0
A_{30}	34816	126	22	943	0	0	0
A_{32}	114563	261	189	0	0	0	0

We have

$$A_i(S_2) \equiv 5 \times A_i(H_2) - 2 \times A_i(G_4^0) - 2 \times A_i(G_4^1) \pmod 8 ,$$

for $\hat{\mathscr{L}}_{137}$, which is identical to that for $\hat{\mathscr{L}}_{167}$ since they both have 2^3 as the highest power of 2 that divides $|\mathscr{H}|$. Using this formulation, we obtain

$$
\begin{aligned}
A_{22}(S_2) &= 2 \pmod 8 \\
A_{24}(S_2) &= 4 \pmod 8 \\
A_{26}(S_2) &= 6 \pmod 8 \\
A_{28}(S_2) &= 2 \pmod 8 \\
A_{30}(S_2) &= 0 \pmod 8 \\
A_{32}(S_2) &= 3 \pmod 8
\end{aligned}
$$

and combining all the results using the Chinese remainder theorem, we arrive at

$$\begin{aligned} A_{22} &= n_{22} \times 1285608 + 321402 \\ A_{24} &= n_{24} \times 1285608 + 1071340 \\ A_{26} &= n_{26} \times 1285608 + 964206 \\ A_{28} &= n_{28} \times 1285608 + 321402 \\ A_{30} &= n_{30} \times 1285608 + 428536 \\ A_{32} &= n_{32} \times 1285608 + 1124907 \end{aligned} \tag{9.44}$$

for some non-negative integers n_i. Comparing these to the results in [4], we can immediately see that $n_{22} = 0$, $n_{24} = 1$, $n_{26} = 16$, $n_{28} = 381$, and both A_{30} and A_{32} were incorrectly reported. By codeword enumeration using multiple computers in parallel, we have determined that

$$\begin{aligned} A_{30} &= 6648307504 \\ A_{32} &= 77865259035 \end{aligned}$$

hence, referring to (9.44) it is found that $n_{30} = 5171$ and $n_{32} = 60566$.

Example 9.5 Gaborit et al. [4] also published the weight distribution of $\hat{\mathscr{L}}_{151}$ and we will show that this has also been incorrectly reported. For $\hat{\mathscr{L}}_{151}$, $|\mathrm{PSL}_2(151)| = 2^3 \times 3 \times 5^2 \times 19 \times 151 = 1721400$ and we have $P = \left[\begin{smallmatrix} 104 & 31 \\ 31 & 47 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 150 \\ 1 & 0 \end{smallmatrix}\right]$.

Let $\left[\begin{smallmatrix} 0 & 1 \\ 150 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 150 & 27 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 150 & 8 \end{smallmatrix}\right]$ be generators of permutation of orders 3, 5 and 19, respectively. The numbers of weight i codewords for $i = 20$ and 24, in the various fixed subcodes of dimension k, are

	H_2	G_4^0	G_4^1	S_3	S_5	S_{19}	S_{151}
k	38	20	19	26	16	4	1
A_{20}	38	2	0	25	15	0	0
A_{24}	266	4	4	100	0	0	0

and $A_i(S_2)$ is again the same as that for primes 167 and 137, see (9.41). Using this equation, we have $A_{20}(S_2) = A_{24}(S_2) = 2 \pmod 8$. Following the Chinese remainder theorem, we obtain

$$\begin{aligned} A_{20} &= n_{20} \times 1721400 + 28690 \\ A_{24} &= n_{24} \times 1721400 + 717250 \end{aligned}. \tag{9.45}$$

It follows that A_{20} is correctly reported in [4], but A_{24} is incorrectly reported as 717230. Using the method in Sect. 9.5 implemented on multiple computers, we have determined that

$$\begin{aligned} A_{20} &= 28690 \\ A_{24} &= 717250, \end{aligned}$$

hence $n_{20} = 0$ and $n_{24} = 0$ in (9.45). Since A_{20} and A_{24} are required to derive the complete weight distribution of $\hat{\mathscr{L}}_{151}$ according to Gleason's theorem for Type-II codes (9.36), the weight distribution of $\hat{\mathscr{L}}_{151}$ given in [4] is not correct. The correct weight distribution of this code, given in terms of the weight enumerator function, is

$$\begin{aligned} A(z) = &\left(z^0 + z^{152}\right) + \\ &28690 \times \left(z^{20} + z^{132}\right) + \\ &717250 \times \left(z^{24} + z^{128}\right) + \\ &164250250 \times \left(z^{28} + z^{124}\right) + \\ &39390351505 \times \left(z^{32} + z^{120}\right) + \\ &5498418962110 \times \left(z^{36} + z^{116}\right) + \\ &430930711621830 \times \left(z^{40} + z^{112}\right) + \\ &19714914846904500 \times \left(z^{44} + z^{108}\right) + \\ &542987434093298550 \times \left(z^{48} + z^{104}\right) + \\ &9222363801696269658 \times \left(z^{52} + z^{100}\right) + \\ &98458872937331749615 \times \left(z^{56} + z^{96}\right) + \\ &670740325520798111830 \times \left(z^{60} + z^{92}\right) + \\ &2949674479653615754525 \times \left(z^{64} + z^{88}\right) + \\ &844602559248350682415 0 \times \left(z^{68} + z^{84}\right) + \\ &158405647602392382324 20 \times \left(z^{72} + z^{80}\right) + \\ &195273646590066972653 68 \times z^{76}. \end{aligned} \tag{9.46}$$

9.7 Minimum Distance Evaluation: A Probabilistic Approach

An interesting observation is that the minimum weight codewords of $\hat{\mathscr{L}}_p$, for $p \equiv \pm 1 \pmod 8$, and $\mathscr{B}_p$, for $p \equiv \pm 3 \pmod 8$ are always contained in one or more of their fixed subcodes. At least, this is true for all known cases ($n \leq 200$) and this is depicted in Table 9.4. We can see that the subcode fixed by H_2 appears in all the known cases. In Table 9.4, the column d_U denotes the minimum distance upper bound of extremal doubly even self-dual codes of a given length and the last column indicates the various subgroups whose fixed subcodes contain the minimum weight codewords. The highest n, for which the minimum distance of extended QR codes is known, is 168 [5] and we provide further results for $n = 192, 194,$ and 200. We obtained the minimum distance of these extended QR codes using the parallel version of the minimum distance algorithm for cyclic codes (QR codes are cyclic) described in Chap. 5, Sect. 5.4. Note that the fact that the code is singly even ($n = 194$) or doubly

Table 9.4 The minimum distance of $\hat{\mathscr{L}}_p$ and $\mathscr{B}_p$ for $12 \le n \le 200$

n	p	p mod 8	d	d_U	Subgroups
12	5	−3	4		H_2, G_4
18	17	1	6		H_2, G_4^0, S_3
24	23	−1	8	8	H_2, G_4^0, G_4^1
28	13	−3	6		H_2, G_4, S_3
32	31	−1	8	8	H_2, G_4^0, S_3
40	19	3	8	8	H_2, G_4, S_3
42	41	1	10		H_2, G_4^1, S_5
48	47	−1	12	12	H_2, G_4^1, S_5
60	29	−3	12		H_2, S_3
72	71	−1	12	16	H_2, G_4^1, S_3, S_5
74	73	1	14		H_2, G_4^0, G_4^1, S_3
76	37	−3	12		H_2, G_4, S_3
80	79	−1	16	16	H_2, G_4^0, G_4^1, S_3
88	43	3	16	16	H_2, S_3, S_7
90	89	1	18		H_2, G_4^0, G_4^1, S_3
98	97	1	16		H_2, G_4^0
104	103	−1	20	20	H_2, G_4^0, S_3
108	53	−3	20		H_2, G_4
114[a]	113	1	16		H_2, G_4^1, S_7
120	59	3	20	24	H_2, G_4, S_5
124	61	−3	20		H_2, G_4, S_3, S_5
128	127	−1	20	24	H_2, S_3
136	67	3	24	24	H_2, G_4, S_3, S_{11}
138	137	1	22		H_2, G_4^0, G_4^1
152[a]	151	−1	20	28	H_2, G_4^0, S_3, S_5
168	167	−1	24	32	H_2, G_4^0, G_4^1, S_3
168	83	3	24	32	H_2, G_4, S_3
192	191	−1	28	36	H_2, G_4^1
194	193	1	28		H_2, G_4^1, S_3
200	199	−1	32	36	H_2, G_4^0, G_4^1, S_3

[a]Extended duadic code [12] has higher minimum distance

even ($n = 192, 200$) is also taken into account in order to reduce the number of codewords that need to be enumerated, see Chap. 5, Sects. 5.2.3 and 5.4. This code property is also taken into account for computing the minimum distance of $\mathscr{B}_p$ using the method described in Sect. 9.5.

Based on the above observation, a probabilistic approach to minimum distance evaluation is developed. Given $\hat{\mathscr{L}}_p$ or $\mathscr{B}_p$, the minimum distance of the code is upper bounded by

$$d \le \min_{Z=\{G_2^0, G_4^0, G_4^1, S_{q_1}, S_{q_2}, \ldots\}} \{d(Z)\}, \tag{9.47}$$

Table 9.5 The minimum distance of $\hat{\mathscr{L}}_p$ and $\mathscr{B}_p$ for $204 \leq n \leq 450$

n	p	p mod 8	d	d_U	Subgroups
203	101	−3	≤ 24		H_2, G_4, S_5
216	107	3	≤ 24	40	H_2, G_4, S_3
220	109	−3	≤ 30		H_2, S_3
224	223	−1	≤ 32	40	H_2, G_4^0, G_4^1
234[a]	233	1	≤ 26		H_2, S_{13}
240[b]	239	−1	≤ 32	44	H_2, G_4^1
242[b]	241	1	≤ 32		H_2, G_4^1, S_3, S_5
258[b]	257	1	≤ 34		H_2, G_4^1
264[b]	263	−1	≤ 36	48	H_2, G_4^0, S_3
264[b]	131	3	≤ 40	48	H_2, G_4
272[b]	271	−1	≤ 40	48	H_2, G_4^0, G_4^1, S_3
280[b]	139	3	≤ 36	48	H_2, S_3
282[b]	281	1	≤ 36		H_2, G_4^0, G_4^1, S_3
300[b]	149	−3	≤ 36		H_2, G_4
312[b]	311	−1	≤ 36	56	H_2, G_4^0, S_3
314[b]	313	1	≤ 40		H_2, G_4^1, S_3
316[b]	157	−3	≤ 40		H_2, S_3
328[b]	163	3	≤ 44	56	H_2, G_4
338[b]	337	1	≤ 40		H_2, G_4^1, S_3
348[b]	173	−3	≤ 42		H_2, S_3
354[b]	353	1	≤ 42		H_2, G_4^1
360[b]	359	−1	≤ 40	64	H_2, G_4^0, G_4^1, Z_5
360[b]	179	3	≤ 40	64	H_2, G_4, Z_5
364[b]	181	−3	≤ 40		H_2, G_4, Z_3
368[b]	367	−1	≤ 48	64	$H_2, G_4^0, Z_3,$
384[b]	383	−1	≤ 48	68	H_2, G_4^0, Z_3
396[b]	197	−3	≤ 44		H_2, Z_{11}
402[b]	201	1	≤ 42		H_2, G_4^0, G_4^1, Z_5
410[b]	409	1	≤ 48		H_2, G_4^0, Z_3
424[b]	211	3	≤ 56	72	H_2, G_4, Z_3, Z_7
432[b]	431	−1	≤ 48	76	H_2, G_4^0, G_4^1, Z_3
434[b]	433	1	≤ 38		H_2, G_4^0, Z_3
440[b]	440	−1	≤ 48	76	H_2, G_4^0, G_4^1, Z_3
450[b]	449	1	≤ 56		H_2, G_4^1

[a]Extended duadic code [12] has higher minimum distance
[b]The minimum distance of the subcode is computed probabilistically

where $d(Z)$ is the minimum distance of the subcode fixed by $Z \in \mathrm{PSL}_2(p)$ and q runs through all odd primes that divide $|\mathrm{PSL}_2(p)|$. Note that for $\mathscr{B}_p$, $G_4^0 = G_4^1$ hence, only one is required. Using (9.47), we give an upper bound of the minimum distance of $\hat{\mathscr{L}}_p$ and $\mathscr{B}_p$ for all codes where $n \leq 450$ and this is tabulated in Table 9.5. The

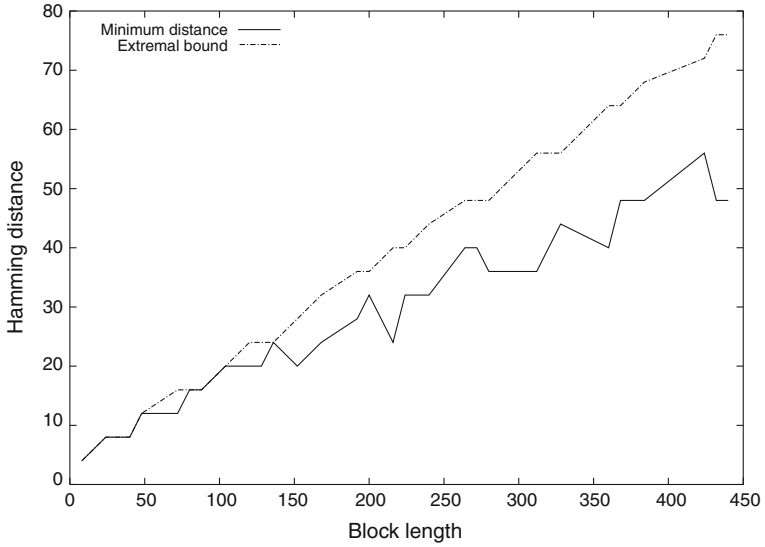

Fig. 9.1 Minimum distance and the extremal bound for distance of doubly even self-dual codes

various fixed subgroups where the minimum weight codewords are found are given in the last column of this table. As shown in Tables 9.4 and 9.5, there is no extremal extended QR or quadratic double-circulant codes for $136 < n \leq 450$ and we plot the minimum distance (or its upper bound for $n > 200$) against the extremal bound in Fig. 9.1. From this figure, it is obvious that, as the block length increases, the gap between the extremal bound and the minimum distance widens and it seems that longer block lengths will follow the same trend. Thus, we conjecture that $n = 136$ is the longest doubly even extremal self-dual double-circulant code. It is worth noting that, for extended QR codes, the results obtained using this probabilistic method are the same as those published by Leon [11].

9.8 Conclusions

Bordered double-circulant codes based on primes can be classified into two classes: $(p + 1, (p + 1)/2, d)$ extended QR codes, for primes $\pm 1 \pmod 8$, and $(2(p + 1), p + 1, d)$ quadratic double-circulant codes, for primes $\pm 3 \pmod 8$.

Whilst quadratic double-circulant codes always exist, given a prime $p \equiv \pm 3 \pmod 8$, bordered double-circulant codes may not exist given a prime $p \equiv \pm 1 \pmod 8$.

There always exist $(2p, p, d)$ pure double-circulant codes for any prime $p \equiv \pm 3 \pmod 8$.

For primes $p \equiv -1, 3 \pmod 8$, the double-circulant codes are self-dual and for other primes, the double-circulant codes are formally self-dual.

By exploiting the code structure of formally self-dual, double-circulant codes for $p \equiv -3 \pmod 8$ and also the self-dual double-circulant codes for both pure and bordered cases, we have shown that, compared to the standard method of evaluation, the number of codewords required to evaluate the minimum distance or to count the number of codewords of a given weight can be reduced by a factor of 2.

The automorphism group of the $(p + 1, (p + 1)/2, d)$ extended QR code contains the projective special linear group $\mathrm{PSL}_2(p)$ acting on the coordinates $(\infty)(0, 1, \ldots, p - 2, p - 1)$.

The automorphism group of the $(2(p + 1), p + 1, d)$ quadratic double-circulant code contains $\mathrm{PSL}_2(p)$, acting on coordinates $(\infty)(0, 1, \ldots, p - 2, p - 1)$, applied simultaneously to left and right circulants.

The number of codewords of weight i of prime-based double-circulant codes, denoted by A_i, can be written as $A_i = n_i \times |\mathrm{PSL}_2(p)| + A_i(\mathrm{PSL}_2(p)) \equiv A_i(\mathrm{PSL}_2(p)) \pmod{|\mathrm{PSL}_2(p)|}$ where $A_i(\mathrm{PSL}_2(p))$ denotes the number of codewords of weight i that are fixed by some element of $\mathrm{PSL}_2(p)$. This result was due to Mykkeltveit et al. [14] and was originally introduced for extended QR codes. We have shown in this chapter that, with some modifications, this modulo congruence method can also be applied to quadratic double-circulant codes.

The modulo congruence technique is found to be very useful in verifying the number of codewords of a given weight obtained exhaustively by computation. We have shown the usefulness of this method by providing corrections to mistakes in previously published results of the weight distributions of extended QR codes for primes 137 and 151.

The weight distribution of the (168, 84, 24) extended QR code, which was previously unknown, has been evaluated and presented above. There also exists a quadratic double-circulant code with identical parameters (n, k and d) and the weight distribution of this code has also been presented above. The (168, 84, 24) quadratic double-circulant code is a better code than the (168, 84, 24) extended QR code since it has less low-weight codewords. The usefulness of the modulo congruence method in checking weight distribution results has been demonstrated in verifying the correctness of the weight distributions of these two codes.

The weight enumerator polynomial of an extended QR code of prime p, denoted by $A_{\hat{\mathscr{Q}}}(z)$, can be obtained using Gleason's theorem once the first few terms are known. Since $\mathrm{PSL}_2(p)$ is doubly transitive [13], knowing $A_{\hat{\mathscr{Q}}}(z)$ implies $A_{\mathscr{Q}}(z)$, the weight enumerator polynomial of the corresponding cyclic QR code, is also known, i.e.

$$A_{\mathscr{Q}}(z) = A_{\hat{\mathscr{Q}}}(z) + \frac{1 - z}{p + 1} A'_{\hat{\mathscr{Q}}}(z)$$

where $A'_{\mathscr{L}}(z)$ is the first derivative of $A_{\mathscr{L}}(z)$ with the respect to z [19]. As a consequence, we have been able to evaluate the weight distributions of the QR codes for primes 151 and 167. These are tabulated in Appendix "Weight Distributions of Quadratic Residues Codes for Primes 151 and 167", Tables 9.19 and 9.20, respectively.

A new probabilistic method to obtain the minimum distance of double-circulant codes based on primes has been described. This probabilistic approach is based on the observation that the minimum weight codewords are always contained in one or more subcodes fixed by some element of $\mathrm{PSL}_2(p)$. Using this approach, we conjecture that there are no extremal double-circulant self-dual codes longer than 136 and that this is the last extremal code to be found.

9.9 Summary

In this chapter, self-dual and binary double-circulant codes based on primes have been described in detail. These binary codes are some of the most powerful codes known and as such form an important class of codes due to their powerful error-correcting capabilities and their rich mathematical structure. This structure enables the entire weight distribution of a code to be determined. With these properties, this family of codes has been a subject of extensive research for many years. For these codes that are longer than around 150 bits, an accurate determination of the codeword weight distributions has been an unsolved challenge. We have shown that the code structure may be used in a new algorithm that requires less codewords to be enumerated than traditional methods. As a consequence we have presented new weight distribution results for codes of length 152, 168, 192, 194 and 200. We have shown how a modular congruence method can be used to check weight distributions and have corrected some mistakes in previously published results for codes of lengths 137 and 151. For evaluation of the minimum Hamming distance for very long codes a new probabilistic method has been presented along with results for codes up to 450 bits long. It is conjectured that the (136, 68, 24) self-dual code is the longest extremal code, meeting the upper bound for minimum Hamming distance, and no other, longer, extremal code exists.

Appendix

Circulant Analysis $p = 11$

See Tables 9.6, 9.7 and 9.8.

Table 9.6 Circulant analysis $p = 11$, $a(x) = 1 + x + x^3$, non-factors of $1 + x^p$

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
1	0, 1, 3	2	0, 2, 6	3	0, 1, 2, 5, 6, 7, 9	4	0, 1, 4	5	0, 2, 3, 5, 7
6	0, 1, 2, 3, 4, 7, 10	7	2, 3, 4, 6, 8	8	0, 2, 8	9	1, 2, 5, 8, 9	10	0, 3, 4, 6, 10
11	1, 2, 5, 9, 10	12	0, 2, 3, 4, 6, 8, 9	13	2, 3, 8, 9, 10	14	1, 4, 5, 6, 8	15	0, 1, 2
16	0, 4, 5	17	0, 1, 3, 4, 6, 7, 8	18	2, 4, 5, 7, 10	19	0, 3, 4, 5, 6	20	0, 1, 6, 8, 9
21	1, 2, 3, 4, 6, 7, 8, 9, 10	22	2, 4, 7, 9, 10	23	0, 1, 3, 4, 8, 9, 10	24	0, 1, 4, 5, 6, 7, 8	25	2, 3, 7, 8, 10
26	4, 5, 6, 7, 9	27	1, 4, 7	28	1, 2, 5, 8, 10	29	1, 2, 3, 4, 6, 9, 10	30	0, 2, 4
31	0, 1, 2, 4, 7	32	0, 8, 10	33	0, 1, 2, 3, 8, 9, 10	34	0, 1, 2, 3, 5, 6, 8	35	3, 6, 7
36	3, 4, 8, 9, 10	37	1, 2, 3, 5, 6, 7, 8	38	0, 1, 6, 8, 10	39	0, 3, 4, 6, 7, 8, 10	40	0, 1, 2, 5, 7
41	0, 4, 6, 7, 10	42	1, 2, 3, 4, 5, 6, 7, 8, 9	43	0, 4, 5, 6, 7, 8, 9	44	3, 4, 7, 8, 9	45	0, 1, 3, 5, 6
46	0, 2, 5, 6, 7, 8, 9	47	2, 8, 9	48	0, 1, 2, 3, 5, 8, 10	49	0, 2, 3, 9, 10	50	3, 4, 5, 6, 9
51	1, 3, 6, 8, 10	52	1, 3, 7, 8, 10	53	1, 3, 6, 7, 9	54	2, 3, 8	55	0, 2, 4, 5, 6, 8, 9
56	2, 4, 5, 9, 10	57	0, 1, 3, 4, 5, 6, 7, 8, 9	58	1, 2, 4, 6, 7, 8, 9	59	0, 3, 6, 7, 9	60	0, 4, 8
61	1, 3, 4, 5, 7, 8, 9	62	0, 2, 3, 4, 8	63	1, 2, 3, 6, 7, 8, 9	64	0, 5, 9	65	0, 3, 5, 6, 8, 9, 10
66	0, 2, 4, 5, 6, 7, 9	67	0, 2, 4, 5, 7	68	0, 1, 2, 4, 5, 6, 10	69	2, 5, 8, 9, 10	70	1, 3, 6
71	1, 2, 3, 7, 9	72	5, 6, 7, 8, 9	73	0, 1, 5, 8, 9	74	1, 2, 3, 4, 5, 6, 10	75	0, 1, 2, 4, 5, 6, 8, 9, 10
76	0, 1, 2, 5, 9	77	0, 1, 4, 6, 8, 9, 10	78	0, 1, 3, 5, 6, 8, 9	79	1, 2, 5, 6, 7, 9, 10	80	0, 2, 3, 4, 10
81	1, 3, 6, 7, 10	82	0, 1, 3, 8, 9	83	1, 2, 6, 8, 10	84	1, 2, 3, 4, 5, 6, 7, 8, 10	85	1, 2, 4, 5, 6, 7, 8
86	0, 1, 3, 5, 7, 8, 10	87	0, 5, 7, 8, 9	88	3, 5, 6, 7, 8	89	0, 3, 4, 5, 6, 8, 10	90	0, 1, 2, 6, 10
91	2, 4, 5, 6, 7, 9, 10	92	0, 1, 3, 4, 5, 7, 10	93	4	94	4, 5, 7	95	4, 6, 10
96	0, 2, 4, 5, 6, 9, 10	97	4, 5, 8	98	0, 4, 6, 7, 9	99	0, 3, 4, 5, 6, 7, 8	100	1, 6, 7, 8, 10
101	1, 4, 6	102	1, 2, 5, 6, 9	103	3, 4, 7, 8, 10	104	2, 3, 5, 6, 9	105	1, 2, 4, 6, 7, 8, 10
106	1, 2, 3, 6, 7	107	1, 5, 8, 9, 10	108	4, 5, 6	109	4, 8, 9	110	0, 1, 4, 5, 7, 8, 10
111	0, 3, 6, 8, 9	112	4, 7, 8, 9, 10	113	1, 2, 4, 5, 10	114	0, 1, 2, 3, 5, 6, 7, 8, 10	115	0, 2, 3, 6, 8
116	1, 2, 3, 4, 5, 7, 8	117	0, 1, 4, 5, 8, 9, 10	118	0, 1, 3, 6, 7	119	0, 2, 8, 9, 10	120	0, 5, 8

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
121	1, 3, 5, 6, 9	122	2, 3, 5, 6, 7, 8, 10	123	4, 6, 8	124	0, 4, 5, 6, 8	125	1, 3, 4
126	1, 2, 3, 4, 5, 6, 7	127	1, 4, 5, 6, 7, 9, 10	128	0, 7, 10	129	1, 2, 3, 7, 8	130	0, 1, 5, 6, 7, 9, 10
131	1, 3, 4, 5, 10	132	0, 1, 3, 4, 7, 8, 10	133	0, 4, 5, 6, 9	134	0, 3, 4, 8, 10	135	0, 1, 2, 5, 6, 7, 8, 9, 10
136	0, 1, 2, 4, 8, 9, 10	137	0, 1, 2, 7, 8	138	4, 5, 7, 9, 10	139	0, 1, 2, 4, 6, 9, 10	140	1, 2, 6
141	1, 3, 4, 5, 6, 7, 9	142	2, 3, 4, 6, 7	143	2, 7, 8, 9, 10	144	1, 3, 5, 7, 10	145	0, 1, 3, 5, 7
146	0, 2, 5, 7, 10	147	1, 6, 7	148	1, 2, 4, 6, 8, 9, 10	149	2, 3, 6, 8, 9	150	0, 1, 2, 4, 5, 7, 8, 9, 10
151	0, 1, 2, 5, 6, 8, 10	152	0, 2, 4, 7, 10	153	1, 4, 8	154	0, 1, 2, 5, 7, 8, 9	155	1, 4, 6, 7, 8
156	0, 1, 2, 5, 6, 7,10	157	2, 4,9	158	1, 2, 3, 4, 7, 9, 10	159	0, 2, 4, 6, 8, 9, 10	160	0, 4, 6, 8,9
161	3, 4,5, 6,8, 9,10	162	1, 2, 3, 6, 9	163	5, 7, 10	164	0, 2,5, 6,7	165	0, 1,2, 9,10
166	1, 2,4, 5,9	167	3, 5,6, 7,8, 9,10	168	1, 2,3, 4,5, 6,8, 9,10	169	2, 4, 5, 6,9	170	1, 2, 3, 4, 5, 8,10
171	1, 2,4, 5,7, 9,10	172	0, 2,3, 5,6, 9,10	173	3, 4, 6, 7,8	174	0, 3,5, 7, 10	175	1, 2, 4, 5,7
176	1, 3,5, 6,10	177	0, 1,3, 5,6, 7,8, 9,10	178	0, 1, 5, 6,8, 9,10	179	0, 1, 3, 4, 5, 7, 9	180	0, 1,2, 4,9
181	0, 1,7, 9,10	182	1, 3,4, 7,8, 9,10	183	3, 4, 5, 6, 10	184	0, 2, 3, 6, 8, 9,10	185	0, 3, 4, 5, 7, 8,9
186	8	187	0, 8,9	188	3, 8,10	189	2, 3, 4, 6, 8, 9, 10	190	1, 8, 9
191	0, 2, 4, 8, 10	192	0, 1, 4, 7, 8, 9, 10	193	0, 1, 3, 5, 10	194	5, 8, 10	195	2, 5, 6, 9, 10
196	0, 1, 3, 7, 8	197	2, 6, 7, 9, 10	198	0, 1, 3, 5, 6, 8, 10	199	0, 5, 6, 7, 10	200	1, 2, 3, 5, 9
201	8, 9, 10	202	1, 2, 8	203	0, 1, 3, 4, 5, 8, 9	204	1, 2, 4, 7, 10	205	0, 1, 2, 3, 8
206	3, 5, 6, 8, 9	207	0, 1, 3, 4, 5, 6, 7, 9, 10	208	1, 4, 6, 7, 10	209	0, 1, 5, 6, 7, 8, 9	210	1, 2, 3, 4, 5, 8, 9
211	0, 4, 5, 7, 10	212	1, 2, 3, 4, 6	213	1, 4, 9	214	2, 5, 7, 9, 10	215	0, 1, 3, 6, 7, 9, 10
216	1, 8, 10	217	1, 4, 8, 9, 10	218	5, 7, 8	219	0, 5, 6, 7, 8, 9, 10	220	0, 2, 3, 5, 8, 9, 10
221	0, 3, 4	222	0, 1, 5, 6, 7	223	0, 2, 3, 4, 5, 9, 10	224	3, 5, 7, 8, 9	225	0, 1, 3, 4, 5, 7, 8
226	2, 4, 8, 9, 10	227	1, 3, 4, 7, 8	228	0, 1, 2, 3, 4, 5, 6, 9, 10	229	1, 2, 3, 4, 5, 6, 8	230	0, 1, 4, 5, 6
231	0, 2, 3, 8, 9	232	2, 3, 4, 5, 6, 8, 10	233	5, 6, 10	234	0, 2, 5, 7, 8, 9, 10	235	0, 6, 7, 8, 10

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
236	0, 1, 2, 3, 6	237	0, 3, 5, 7, 9	238	0, 4, 5, 7, 9	239	0, 3, 4, 6, 9	240	0, 5, 10
241	1, 2, 3, 5, 6, 8, 10	242	1, 2, 6, 7, 10	243	0, 1, 2, 3, 4, 5, 6, 8, 9	244	1, 3, 4, 5, 6, 9, 10	245	0, 3, 4, 6, 8
246	1, 5, 8	247	0, 1, 2, 4, 5, 6, 9	248	0, 1, 5, 8, 10	249	0, 3, 4, 5, 6, 9, 10	250	2, 6, 8
251	0, 2, 3, 5, 6, 7, 8	252	1, 2, 3, 4, 6, 8, 10	253	1, 2, 4, 8, 10	254	1, 2, 3, 7, 8, 9, 10	255	2, 5, 6, 7, 10
256	0, 3, 9	257	0, 4, 6, 9, 10	258	2, 3, 4, 5, 6	259	2, 5, 6, 8, 9	260	0, 1, 2, 3, 7, 9, 10
261	1, 2, 3, 5, 6, 7, 8, 9, 10	262	2, 6, 8, 9, 10	263	1, 3, 5, 6, 7, 8, 9	264	0, 2, 3, 5, 6, 8, 9	265	2, 3, 4, 6, 7, 9, 10
266	0, 1, 7, 8, 10	267	0, 3, 4, 7, 9	268	0, 5, 6, 8, 9	269	3, 5, 7, 9, 10	270	0, 1, 2, 3, 4, 5, 7, 9, 10
271	1, 2, 3, 4, 5, 9, 10	272	0, 2, 4, 5, 7, 8, 9	273	2, 4, 5, 6, 8	274	0, 2, 3, 4, 5	275	0, 1, 2, 3, 5, 7, 8
276	3, 7, 8, 9, 10	277	1, 2, 3, 4, 6, 7, 10	278	0, 1, 2, 4, 7, 8, 9	279	1	280	1, 2, 4
281	1, 3, 7	282	1, 2, 3, 6, 7, 8, 10	283	1, 2, 5	284	1, 3, 4, 6, 8	285	0, 1, 2, 3, 4, 5, 8
286	3, 4, 5, 7, 9	287	1, 3, 9	288	2, 3, 6, 9, 10	289	0, 1, 4, 5, 7	290	0, 2, 3, 6, 10
291	1, 3, 4, 5, 7, 9, 10	292	0, 3, 4, 9, 10	293	2, 5, 6, 7, 9	294	1, 2, 3	295	1, 5, 6
296	1, 2, 4, 5, 7, 8, 9	297	0, 3, 5, 6, 8	298	1, 4, 5, 6, 7	299	1, 2, 7, 9, 10	300	0, 2, 3, 4, 5, 7, 8, 9, 10
301	0, 3, 5, 8, 10	302	0, 1, 2, 4, 5, 9, 10	303	1, 2, 5, 6, 7, 8, 9	304	0, 3, 4, 8, 9	305	5, 6, 7, 8, 10
306	2, 5, 8	307	0, 2, 3, 6, 9	308	0, 2, 3, 4, 5, 7, 10	309	1, 3, 5	310	1, 2, 3, 5, 8
311	0, 1, 9	312	0, 1, 2, 3, 4, 9, 10	313	1, 2, 3, 4, 6, 7, 9	314	4, 7, 8	315	0, 4, 5, 9, 10
316	2, 3, 4, 6, 7, 8, 9	317	0, 1, 2, 7, 9	318	0, 1, 4, 5, 7, 8, 9	319	1, 2, 3, 6, 8	320	0, 1, 5, 7, 8
321	2, 3, 4, 5, 6, 7, 8, 9, 10	322	1, 5, 6, 7, 8, 9, 10	323	4, 5, 8, 9, 10	324	1, 2, 4, 6, 7	325	1, 3, 6, 7, 8, 9, 10
326	3, 9, 10	327	0, 1, 2, 3, 4, 6, 9	328	0, 1, 3, 4, 10	329	4, 5, 6, 7, 10	330	0, 2, 4, 7, 9
331	0, 2, 4, 8, 9	332	2, 4, 7, 8, 10	333	3, 4, 9	334	1, 3, 5, 6, 7, 9, 10	335	0, 3, 5, 6, 10
336	1, 2, 4, 5, 6, 7, 8, 9, 10	337	2, 3, 5, 7, 8, 9, 10	338	1, 4, 7, 8, 10	339	1, 5, 9	340	2, 4, 5, 6, 8, 9, 10
341	1, 3, 4, 5, 9	342	2, 3, 4, 7, 8, 9, 10	343	1, 6, 10	344	0, 1, 4, 6, 7, 9, 10	345	1, 3, 5, 6, 7, 8, 10
346	1, 3, 5, 6, 8	347	0, 1, 2, 3, 5, 6, 7	348	0, 3, 6, 9, 10	349	2, 4, 7	350	2, 3, 4, 8, 10
351	6, 7, 8, 9, 10	352	1, 2, 6, 9, 10	353	0, 2, 3, 4, 5, 6, 7	354	0, 1, 2, 3, 5, 6, 7, 9, 10	355	1, 2, 3, 6, 10

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
356	0, 1, 2, 5, 7, 9, 10	357	1, 2, 4, 6, 7, 9, 10	358	0, 2, 3, 6, 7, 8, 10	359	0, 1, 3, 4, 5	360	0, 2, 4, 7, 8
361	1, 2, 4, 9, 10	362	0, 2, 3, 7, 9	363	0, 2, 3, 4, 5, 6, 7, 8, 9	364	2, 3, 5, 6, 7, 8, 9	365	0, 1, 2, 4, 6, 8, 9
366	1, 6, 8, 9, 10	367	4, 6, 7, 8, 9	368	0, 1, 4, 5, 6, 7, 9	369	0, 1, 2, 3, 7	370	0, 3, 5, 6, 7, 8, 10
371	0, 1, 2, 4, 5, 6, 8	372	5	373	5, 6, 8	374	0, 5, 7	375	0, 1, 3, 5, 6, 7, 10
376	5, 6, 9	377	1, 5, 7, 8, 10	378	1, 4, 5, 6, 7, 8, 9	379	0, 2, 7, 8, 9	380	2, 5, 7
381	2, 3, 6, 7, 10	382	0, 4, 5, 8, 9	383	3, 4, 6, 7, 10	384	0, 2, 3, 5, 7, 8, 9	385	2, 3, 4, 7, 8
386	0, 2, 6, 9, 10	387	5, 6, 7	388	5, 9, 10	389	0, 1, 2, 5, 6, 8, 9	390	1, 4, 7, 9, 10
391	0, 5, 8, 9, 10	392	0, 2, 3, 5, 6	393	0, 1, 2, 3, 4, 6, 7, 8, 9	394	1, 3, 4, 7, 9	395	2, 3, 4, 5, 6, 8, 9
396	0, 1, 2, 5, 6, 9, 10	397	1, 2, 4, 7, 8	398	0, 1, 3, 9, 10	399	1, 6, 9	400	2, 4, 6, 7, 10
401	0, 3, 4, 6, 7, 8, 9	402	5, 7, 9	403	1, 5, 6, 7, 9	404	2, 4, 5	405	2, 3, 4, 5, 6, 7, 8
406	0, 2, 5, 6, 7, 8, 10	407	0, 1, 8	408	2, 3, 4, 8, 9	409	0, 1, 2, 6, 7, 8, 10	410	0, 2, 4, 5, 6
411	0, 1, 2, 4, 5, 8, 9	412	1, 5, 6, 7, 10	413	0, 1, 4, 5, 9	414	0, 1, 2, 3, 6, 7, 8, 9, 10	415	0, 1, 2, 3, 5, 9, 10
416	1, 2, 3, 8, 9	417	0, 5, 6, 8, 10	418	0, 1, 2, 3, 5, 7, 10	419	2, 3, 7	420	2, 4, 5, 6, 7, 8, 10
421	3, 4, 5, 7, 8	422	0, 3, 8, 9, 10	423	0, 2, 4, 6, 8	424	1, 2, 4, 6, 8	425	0, 1, 3, 6, 8
426	2, 7, 8	427	0, 2, 3, 5, 7, 9, 10	428	3, 4, 7, 9, 10	429	0, 1, 2, 3, 5, 6, 8, 9, 10	430	0, 1, 2, 3, 6, 7, 9
431	0, 1, 3, 5, 8	432	2, 5, 9	433	1, 2, 3, 6, 8, 9, 10	434	2, 5, 7, 8, 9	435	0, 1, 2, 3, 6, 7, 8
436	3, 5, 10	437	0, 2, 3, 4, 5, 8, 10	438	0, 1, 3, 5, 7, 9, 10	439	1, 5, 7, 9, 10	440	0, 4, 5, 6, 7, 9, 10
441	2, 3, 4, 7, 10	442	0, 6, 8	443	1, 3, 6, 7, 8	444	0, 1, 2, 3, 10	445	2, 3, 5, 6, 10
446	0, 4, 6, 7, 8, 9, 10	447	0, 2, 3, 4, 5, 6, 7, 9, 10	448	3, 5, 6, 7, 10	449	0, 2, 3, 4, 5, 6, 9	450	0, 2, 3, 5, 6, 8, 10
451	0, 1, 3, 4, 6, 7, 10	452	4, 5, 7, 8, 9	453	0, 1, 4, 6, 8	454	2, 3, 5, 6, 8	455	0, 2, 4, 6, 7
456	0, 1, 2, 4, 6, 7, 8, 9, 10	457	0, 1, 2, 6, 7, 9, 10	458	1, 2, 4, 5, 6, 8, 10	459	1, 2, 3, 5, 10	460	0, 1, 2, 8, 10
461	0, 2, 4, 5, 8, 9, 10	462	0, 4, 5, 6, 7	463	0, 1, 3, 4, 7, 9, 10	464	1, 4, 5, 6, 8, 9, 10	465	9

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
466	1, 9, 10	467	0, 4, 9	468	0, 3, 4, 5, 7, 9, 10	469	2, 9, 10	470	0, 1, 3, 5, 9
471	0, 1, 2, 5, 8, 9, 10	472	0, 1, 2, 4, 6	473	0, 6, 9	474	0, 3, 6, 7, 10	475	1, 2, 4, 8, 9
476	0, 3, 7, 8, 10	477	0, 1, 2, 4, 6, 7, 9	478	0, 1, 6, 7, 8	479	2, 3, 4, 6, 10	480	0, 9, 10
481	2, 3, 9	482	1, 2, 4, 5, 6, 9, 10	483	0, 2, 3, 5, 8	484	1, 2, 3, 4, 9	485	4, 6, 7, 9, 10
486	0, 1, 2, 4, 5, 6, 7, 8, 10	487	0, 2, 5, 7, 8	488	1, 2, 6, 7, 8, 9, 10	489	2, 3, 4, 5, 6, 9, 10	490	0, 1, 5, 6, 8
491	2, 3, 4, 5, 7	492	2, 5, 10	493	0, 3, 6, 8, 10	494	0, 1, 2, 4, 7, 8, 10	495	0, 2, 9
496	0, 2, 5, 9, 10	497	6, 8, 9	498	0, 1, 6, 7, 8, 9, 10	499	0, 1, 3, 4, 6, 9, 10	500	1, 4, 5
501	1, 2, 6, 7, 8	502	0, 1, 3, 4, 5, 6, 10	503	4, 6, 8, 9, 10	504	1, 2, 4, 5, 6, 8, 9	505	0, 3, 5, 9, 10
506	2, 4, 5, 8, 9	507	0, 1, 2, 3, 4, 5, 6, 7, 10	508	2, 3, 4, 5, 6, 7, 9	509	1, 2, 5, 6, 7	510	1, 3, 4, 9, 10
511	0, 3, 4, 5, 6, 7, 9	512	0, 6, 7	513	0, 1, 3, 6, 8, 9, 10	514	0, 1, 7, 8, 9	515	1, 2, 3, 4, 7
516	1, 4, 6, 8, 10	517	1, 5, 6, 8, 10	518	1, 4, 5, 7, 10	519	0, 1, 6	520	0, 2, 3, 4, 6, 7, 9
521	0, 2, 3, 7, 8	522	1, 2, 3, 4, 5, 6, 7, 9, 10	523	0, 2, 4, 5, 6, 7, 10	524	1, 4, 5, 7, 9	525	2, 6, 9
526	1, 2, 3, 5, 6, 7, 10	527	0, 1, 2, 6, 9	528	0, 1, 4, 5, 6, 7, 10	529	3, 7, 9	530	1, 3, 4, 6, 7, 8, 9
531	0, 2, 3, 4, 5, 7, 9	532	0, 2, 3, 5, 9	533	0, 2, 3, 4, 8, 9, 10	534	0, 3, 6, 7, 8	535	1, 4, 10
536	0, 1, 5, 7, 10	537	3, 4, 5, 6, 7	538	3, 6, 7, 9, 10	539	0, 1, 2, 3, 4, 8, 10	540	0, 2, 3, 4, 6, 7, 8, 9, 10
541	0, 3, 7, 9, 10	542	2, 4, 6, 7, 8, 9, 10	543	1, 3, 4, 6, 7, 9, 10	544	0, 3, 4, 5, 7, 8, 10	545	0, 1, 2, 8, 9
546	1, 4, 5, 8, 10	547	1, 6, 7, 9, 10	548	0, 4, 6, 8, 10	549	0, 1, 2, 3, 4, 5, 6, 8, 10	550	0, 2, 3, 4, 5, 6, 10
551	1, 3, 5, 6, 8, 9, 10	552	3, 5, 6, 7, 9	553	1, 3, 4, 5, 6	554	1, 2, 3, 4, 6, 8, 9	555	0, 4, 8, 9, 10
556	0, 2, 3, 4, 5, 7, 8	557	1, 2, 3, 5, 8, 9, 10	558	2	559	2, 3, 5	560	2, 4, 8
561	0, 2, 3, 4, 7, 8, 9	562	2, 3, 6	563	2, 4, 5, 7, 9	564	1, 2, 3, 4, 5, 6, 9	565	4, 5, 6, 8, 10
566	2, 4, 10	567	0, 3, 4, 7, 10	568	1, 2, 5, 6, 8	569	0, 1, 3, 4, 7	570	0, 2, 4, 5, 6, 8, 10

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
571	0, 1, 4, 5, 10	572	3, 6, 7, 8, 10	573	2, 3, 4	574	2, 6, 7	575	2, 3, 5, 6, 8, 9, 10
576	1, 4, 6, 7, 9	577	2, 5, 6, 7, 8	578	0, 2, 3, 8, 10	579	0, 1, 3, 4, 5, 6, 8, 9, 10	580	0, 1, 4, 6, 9
581	0, 1, 2, 3, 5, 6, 10	582	2, 3, 6, 7, 8, 9, 10	583	1, 4, 5, 9, 10	584	0, 6, 7, 8, 9	585	3, 6, 9
586	1, 3, 4, 7, 10	587	0, 1, 3, 4, 5, 6, 8	588	2, 4, 6	589	2, 3, 4, 6, 9	590	1, 2, 10
591	0, 1, 2, 3, 4, 5, 10	592	2, 3, 4, 5, 7, 8, 10	593	5, 8, 9	594	0, 1, 5, 6, 10	595	3, 4, 5, 7, 8, 9, 10
596	1, 2, 3, 8, 10	597	1, 2, 5, 6, 8, 9, 10	598	2, 3, 4, 7, 9	599	1, 2, 6, 8, 9	600	0, 3, 4, 5, 6, 7, 8, 9, 10
601	0, 2, 6, 7, 8, 9, 10	602	0, 5, 6, 9, 10	603	2, 3, 5, 7, 8	604	0, 2, 4, 7, 8, 9, 10	605	0, 4, 10
606	1, 2, 3, 4, 5, 7, 10	607	0, 1, 2, 4, 5	608	0, 5, 6, 7, 8	609	1, 3, 5, 8, 10	610	1, 3, 5, 9, 10
611	0, 3, 5, 8, 9	612	4, 5, 10	613	0, 2, 4, 6, 7, 8, 10	614	0, 1, 4, 6, 7	615	0, 2, 3, 5, 6, 7, 8, 9, 10
616	0, 3, 4, 6, 8, 9, 10	617	0, 2, 5, 8, 9	618	2, 6, 10	619	0, 3, 5, 6, 7, 9, 10	620	2, 4, 5, 6, 10
621	0, 3, 4, 5, 8, 9, 10	622	0, 2, 7	623	0, 1, 2, 5, 7, 8, 10	624	0, 2, 4, 6, 7, 8, 9	625	2, 4, 6, 7, 9
626	1, 2, 3, 4, 6, 7, 8	627	0, 1, 4, 7, 10	628	3, 5, 8	629	0, 3, 4, 5, 9	630	0, 7, 8, 9, 10
631	0, 2, 3, 7, 10	632	1, 3, 4, 5, 6, 7, 8	633	0, 1, 2, 3, 4, 6, 7, 8, 10	634	0, 2, 3, 4, 7	635	0, 1, 2, 3, 6, 8, 10
636	0, 2, 3, 5, 7, 8, 10	637	0, 1, 3, 4, 7, 8, 9	638	1, 2, 4, 5, 6	639	1, 3, 5, 8, 9	640	0, 2, 3, 5, 10
641	1, 3, 4, 8, 10	642	1, 3, 4, 5, 6, 7, 8, 9, 10	643	3, 4, 6, 7, 8, 9, 10	644	1, 2, 3, 5, 7, 9, 10	645	0, 2, 7, 9, 10
646	5, 7, 8, 9, 10	647	1, 2, 5, 6, 7, 8, 10	648	1, 2, 3, 4, 8	649	0, 1, 4, 6, 7, 8, 9	650	1, 2, 3, 5, 6, 7, 9
651	6	652	6, 7, 9	653	1, 6, 8	654	0, 1, 2, 4, 6, 7, 8	655	6, 7, 10
656	0, 2, 6, 8, 9	657	2, 5, 6, 7, 8, 9, 10	658	1, 3, 8, 9, 10	659	3, 6, 8	660	0, 3, 4, 7, 8
661	1, 5, 6, 9, 10	662	0, 4, 5, 7, 8	663	1, 3, 4, 6, 8, 9, 10	664	3, 4, 5, 8, 9	665	0, 1, 3, 7, 10
666	6, 7, 8	667	0, 6, 10	668	1, 2, 3, 6, 7, 9, 10	669	0, 2, 5, 8, 10	670	0, 1, 6, 9, 10
671	1, 3, 4, 6, 7	672	1, 2, 3, 4, 5, 7, 8, 9, 10	673	2, 4, 5, 8, 10	674	3, 4, 5, 6, 7, 9, 10	675	0, 1, 2, 3, 6, 7, 10
676	2, 3, 5, 8, 9	677	0, 1, 2, 4, 10	678	2, 7, 10	679	0, 3, 5, 7, 8	680	1, 4, 5, 7, 8, 9, 10
681	6, 8, 10	682	2, 6, 7, 8, 10	683	3, 5, 6	684	3, 4, 5, 6, 7, 8, 9	685	0, 1, 3, 6, 7, 8, 9
686	1, 2, 9	687	3, 4, 5, 9, 10	688	0, 1, 2, 3, 7, 8, 9	689	1, 3, 5, 6, 7	690	1, 2, 3, 5, 6, 9, 10

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
691	0, 2, 6, 7, 8	692	1, 2, 5, 6, 10	693	0, 1, 2, 3, 4, 7, 8, 9, 10	694	0, 1, 2, 3, 4, 6, 10	695	2, 3, 4, 9, 10
696	0, 1, 6, 7, 9	697	0, 1, 2, 3, 4, 6, 8	698	3, 4, 8	699	0, 3, 5, 6, 7, 8, 9	700	4, 5, 6, 8, 9
701	0, 1, 4, 9, 10	702	1, 3, 5, 7, 9	703	2, 3, 5, 7, 9	704	1, 2, 4, 7, 9	705	3, 8, 9
706	0, 1, 3, 4, 6, 8, 10	707	0, 4, 5, 8, 10	708	0, 1, 2, 3, 4, 6, 7, 9, 10	709	1, 2, 3, 4, 7, 8, 10	710	1, 2, 4, 6, 9
711	3, 6, 10	712	0, 2, 3, 4, 7, 9, 10	713	3, 6, 8, 9, 10	714	1, 2, 3, 4, 7, 8, 9	715	0, 4, 6
716	0, 1, 3, 4, 5, 6, 9	717	0, 1, 2, 4, 6, 8, 10	718	0, 2, 6, 8, 10	719	0, 1, 5, 6, 7, 8, 10	720	0, 3, 4, 5, 8
721	1, 7, 9	722	2, 4, 7, 8, 9	723	0, 1, 2, 3, 4	724	0, 3, 4, 6, 7	725	0, 1, 5, 7, 8, 9, 10
726	0, 1, 3, 4, 5, 6, 7, 8, 10	727	0, 4, 6, 7, 8	728	1, 3, 4, 5, 6, 7, 10	729	0, 1, 3, 4, 6, 7, 9	730	0, 1, 2, 4, 5, 7, 8
731	5, 6, 8, 9, 10	732	1, 2, 5, 7, 9	733	3, 4, 6, 7, 9	734	1, 3, 5, 7, 8	735	0, 1, 2, 3, 5, 7, 8, 9, 10
736	0, 1, 2, 3, 7, 8, 10	737	0, 2, 3, 5, 6, 7, 9	738	0, 2, 3, 4, 6	739	0, 1, 2, 3, 9	740	0, 1, 3, 5, 6, 9, 10
741	1, 5, 6, 7, 8	742	0, 1, 2, 4, 5, 8, 10	743	0, 2, 5, 6, 7, 9, 10	744	10	745	0, 2, 10
746	1, 5, 10	747	0, 1, 4, 5, 6, 8, 10	748	0, 3, 10	749	1, 2, 4, 6, 10	750	0, 1, 2, 3, 6, 9, 10
751	1, 2, 3, 5, 7	752	1, 7, 10	753	0, 1, 4, 7, 8	754	2, 3, 5, 9, 10	755	0, 1, 4, 8, 9
756	1, 2, 3, 5, 7, 8, 10	757	1, 2, 7, 8, 9	758	0, 3, 4, 5, 7	759	0, 1, 10	760	3, 4, 10
761	0, 2, 3, 5, 6, 7, 10	762	1, 3, 4, 6, 9	763	2, 3, 4, 5, 10	764	0, 5, 7, 8, 10	765	0, 1, 2, 3, 5, 6, 7, 8, 9
766	1, 3, 6, 8, 9	767	0, 2, 3, 7, 8, 9, 10	768	0, 3, 4, 5, 6, 7, 10	769	1, 2, 6, 7, 9	770	3, 4, 5, 6, 8
771	0, 3, 6	772	0, 1, 4, 7, 9	773	0, 1, 2, 3, 5, 8, 9	774	1, 3, 10	775	0, 1, 3, 6, 10
776	7, 9, 10	777	0, 1, 2, 7, 8, 9, 10	778	0, 1, 2, 4, 5, 7, 10	779	2, 5, 6	780	2, 3, 7, 8, 9
781	0, 1, 2, 4, 5, 6, 7	782	0, 5, 7, 9, 10	783	2, 3, 5, 6, 7, 9, 10	784	0, 1, 4, 6, 10	785	3, 5, 6, 9, 10
786	0, 1, 2, 3, 4, 5, 6, 7, 8	787	3, 4, 5, 6, 7, 8, 10	788	2, 3, 6, 7, 8	789	0, 2, 4, 5, 10	790	1, 4, 5, 6, 7, 8, 10
791	1, 7, 8	792	0, 1, 2, 4, 7, 9, 10	793	1, 2, 8, 9, 10	794	2, 3, 4, 5, 8	795	0, 2, 5, 7, 9
796	0, 2, 6, 7, 9	797	0, 2, 5, 6, 8	798	1, 2, 7	799	1, 3, 4, 5, 7, 8, 10	800	1, 3, 4, 8, 9
801	0, 2, 3, 4, 5, 6, 7, 8, 10	802	0, 1, 3, 5, 6, 7, 8	803	2, 5, 6, 8, 10	804	3, 7, 10	805	0, 2, 3, 4, 6, 7, 8

(continued)

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
806	1, 2, 3, 7, 10	807	0, 1, 2, 5, 6, 7, 8	808	4, 8, 10	809	2, 4, 5, 7, 8, 9, 10	810	1, 3, 4, 5, 6, 8, 10
811	1, 3, 4, 6, 10	812	0, 1, 3, 4, 5, 9, 10	813	1, 4, 7, 8, 9	814	0, 2, 5	815	0, 1, 2, 6, 8
816	4, 5, 6, 7, 8	817	0, 4, 7, 8, 10	818	0, 1, 2, 3, 4, 5, 9	819	0, 1, 3, 4, 5, 7, 8, 9, 10	820	0, 1, 4, 8, 10
821	0, 3, 5, 7, 8, 9, 10	822	0, 2, 4, 5, 7, 8, 10	823	0, 1, 4, 5, 6, 8, 9	824	1, 2, 3, 9, 10	825	0, 2, 5, 6, 9
826	0, 2, 7, 8, 10	827	0, 1, 5, 7, 9	828	0, 1, 2, 3, 4, 5, 6, 7, 9	829	0, 1, 3, 4, 5, 6, 7	830	0, 2, 4, 6, 7, 9, 10
831	4, 6, 7, 8, 10	832	2, 4, 5, 6, 7	833	2, 3, 4, 5, 7, 9, 10	834	0, 1, 5, 9, 10	835	1, 3, 4, 5, 6, 8, 9
836	0, 2, 3, 4, 6, 9, 10	837	3	838	3, 4, 6	839	3, 5, 9	840	1, 3, 4, 5, 8, 9, 10
841	3, 4, 7	842	3, 5, 6, 8, 10	843	2, 3, 4, 5, 6, 7, 10	844	0, 5, 6, 7, 9	845	0, 3, 5
846	0, 1, 4, 5, 8	847	2, 3, 6, 7, 9	848	1, 2, 4, 5, 8	849	0, 1, 3, 5, 6, 7, 9	850	0, 1, 2, 5, 6
851	0, 4, 7, 8, 9	852	3, 4, 5	853	3, 7, 8	854	0, 3, 4, 6, 7, 9, 10	855	2, 5, 7, 8, 10
856	3, 6, 7, 8, 9	857	0, 1, 3, 4, 9	858	0, 1, 2, 4, 5, 6, 7, 9, 10	859	1, 2, 5, 7, 10	860	0, 1, 2, 3, 4, 6, 7
861	0, 3, 4, 7, 8, 9, 10	862	0, 2, 5, 6, 10	863	1, 7, 8, 9, 10	864	4, 7, 10	865	0, 2, 4, 5, 8
866	1, 2, 4, 5, 6, 7, 9	867	3, 5, 7	868	3, 4, 5, 7, 10	869	0, 2, 3	870	0, 1, 2, 3, 4, 5, 6
871	0, 3, 4, 5, 6, 8, 9	872	6, 9, 10	873	0, 1, 2, 6, 7	874	0, 4, 5, 6, 8, 9, 10	875	0, 2, 3, 4, 9
876	0, 2, 3, 6, 7, 9, 10	877	3, 4, 5, 8, 10	878	2, 3, 7, 9, 10	879	0, 1, 4, 5, 6, 7, 8, 9, 10	880	0, 1, 3, 7, 8, 9, 10
881	0, 1, 6, 7, 10	882	3, 4, 6, 8, 9	883	0, 1, 3, 5, 8, 9, 10	884	0, 1, 5	885	0, 2, 3, 4, 5, 6, 8
886	1, 2, 3, 5, 6	887	1, 6, 7, 8, 9	888	0, 2, 4, 6, 9	889	0, 2, 4, 6, 10	890	1, 4, 6, 9, 10
891	0, 5, 6	892	0, 1, 3, 5, 7, 8, 9	893	1, 2, 5, 7, 8	894	0, 1, 3, 4, 6, 7, 8, 9, 10	895	0, 1, 4, 5, 7, 9, 10
896	1, 3, 6, 9, 10	897	0, 3, 7	898	0, 1, 4, 6, 7, 8, 10	899	0, 3, 5, 6, 7	900	0, 1, 4, 5, 6, 9, 10
901	1, 3, 8	902	0, 1, 2, 3, 6, 8, 9	903	1, 3, 5, 7, 8, 9, 10	904	3, 5, 7, 8, 10	905	2, 3, 4, 5, 7, 8, 9
906	0, 1, 2, 5, 8	907	4, 6, 9	908	1, 4, 5, 6, 10	909	0, 1, 8, 9, 10	910	0, 1, 3, 4, 8
911	2, 4, 5, 6, 7, 8, 9	912	0, 1, 2, 3, 4, 5, 7, 8, 9	913	1, 3, 4, 5, 8	914	0, 1, 2, 3, 4, 7, 9	915	0, 1, 3, 4, 6, 8, 9
916	1, 2, 4, 5, 8, 9, 10	917	2, 3, 5, 6, 7	918	2, 4, 6, 9, 10	919	0, 1, 3, 4, 6	920	0, 2, 4, 5, 9
921	0, 2, 4, 5, 6, 7, 8, 9, 10	922	0, 4, 5, 7, 8, 9, 10	923	0, 2, 3, 4, 6, 8, 10	924	0, 1, 3, 8, 10	925	0, 6, 8, 9, 10
926	0, 2, 3, 6, 7, 8, 9	927	2, 3, 4, 5, 9	928	1, 2, 5, 7, 8, 9, 10	929	2, 3, 4, 6, 7, 8, 10	930	7

Table 9.6 (continued)

i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$	i	$a(x)^i$
931	7, 8, 10	932	2, 7, 9	933	1, 2, 3, 5, 7, 8, 9	934	0, 7, 8	935	1, 3, 7, 9, 10
936	0, 3, 6, 7, 8, 9, 10	937	0, 2, 4, 9, 10	938	4, 7, 9	939	1, 4, 5, 8, 9	940	0, 2, 6, 7, 10
941	1, 5, 6, 8, 9	942	0, 2, 4, 5, 7, 9, 10	943	4, 5, 6, 9, 10	944	0, 1, 2, 4, 8	945	7, 8, 9
946	0, 1, 7	947	0, 2, 3, 4, 7, 8, 10	948	0, 1, 3, 6, 9	949	0, 1, 2, 7, 10	950	2, 4, 5, 7, 8
951	0, 2, 3, 4, 5, 6, 8, 9, 10	952	0, 3, 5, 6, 9	953	0, 4, 5, 6, 7, 8, 10	954	0, 1, 2, 3, 4, 7, 8	955	3, 4, 6, 9, 10
956	0, 1, 2, 3, 5	957	0, 3, 8	958	1, 4, 6, 8, 9	959	0, 2, 5, 6, 8, 9, 10	960	0, 7, 9
961	0, 3, 7, 8, 9	962	4, 6, 7	963	4, 5, 6, 7, 8, 9, 10	964	1, 2, 4, 7, 8, 9, 10	965	2, 3, 10
966	0, 4, 5, 6, 10	967	1, 2, 3, 4, 8, 9, 10	968	2, 4, 6, 7, 8	969	0, 2, 3, 4, 6, 7, 10	970	1, 3, 7, 8, 9
971	0, 2, 3, 6, 7	972	0, 1, 2, 3, 4, 5, 8, 9, 10	973	0, 1, 2, 3, 4, 5, 7	974	0, 3, 4, 5, 10	975	1, 2, 7, 8, 10
976	1, 2, 3, 4, 5, 7, 9	977	4, 5, 9	978	1, 4, 6, 7, 8, 9, 10	979	5, 6, 7, 9, 10	980	0, 1, 2, 5, 10
981	2, 4, 6, 8, 10	982	3, 4, 6, 8, 10	983	2, 3, 5, 8, 10	984	4, 9, 10	985	0, 1, 2, 4, 5, 7, 9
986	0, 1, 5, 6, 9	987	0, 1, 2, 3, 4, 5, 7, 8, 10	988	0, 2, 3, 4, 5, 8, 9	989	2, 3, 5, 7, 10	990	0, 4, 7
991	0, 1, 3, 4, 5, 8, 10	992	0, 4, 7, 9, 10	993	2, 3, 4, 5, 8, 9, 10	994	1, 5, 7	995	1, 2, 4, 5, 6, 7, 10
996	0, 1, 2, 3, 5, 7, 9	997	0, 1, 3, 7, 9	998	0, 1, 2, 6, 7, 8, 9	999	1, 4, 5, 6, 9	1000	2, 8, 10
1001	3, 5, 8, 9, 10	1002	1, 2, 3, 4, 5	1003	1, 4, 5, 7, 8	1004	0, 1, 2, 6, 8, 9, 10	1005	0, 1, 2, 4, 5, 6, 7, 8, 9
1006	1, 5, 7, 8, 9	1007	0, 2, 4, 5, 6, 7, 8	1008	1, 2, 4, 5, 7, 8, 10	1009	1, 2, 3, 5, 6, 8, 9	1010	0, 6, 7, 9, 10
1011	2, 3, 6, 8, 10	1012	4, 5, 7, 8, 10	1013	2, 4, 6, 8, 9	1014	0, 1, 2, 3, 4, 6, 8, 9, 10	1015	0, 1, 2, 3, 4, 8, 9
1016	1, 3, 4, 6, 7, 8, 10	1017	1, 3, 4, 5, 7	1018	1, 2, 3, 4, 10	1019	0, 1, 2, 4, 6, 7, 10	1020	2, 6, 7, 8, 9
1021	0, 1, 2, 3, 5, 6, 9	1022	0, 1, 3, 6, 7, 8, 10	1023	0				

Table 9.7 Circulant analysis $p = 11, \alpha(x) = 1 + x + x^2 + x^4$, factors of $1 + x^p$

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
1	0, 1, 2, 4	2	0, 2, 4, 8	3	0, 3, 4, 5, 9, 10	4	0, 4, 5, 8	5	0, 2, 7, 10
6	0, 6, 7, 8, 9, 10	7	1, 3, 4, 6, 8, 9	8	0, 5, 8, 10	9	1, 2, 3, 4, 5, 6, 7, 8	10	0, 3, 4, 9
11	1, 3, 4, 6, 7, 8, 9, 10	12	0, 1, 3, 5, 7, 9	13	0, 2, 5, 6, 7, 8, 9, 10	14	1, 2, 5, 6, 7, 8	15	0, 4, 6, 7, 8, 9
16	0, 5, 9, 10	17	0, 3, 4, 5, 6, 7	18	1, 2, 3, 4, 5, 6, 8, 10	19	0, 1, 4, 7, 8, 10	20	0, 6, 7, 8
21	2, 4, 6, 8	22	1, 2, 3, 5, 6, 7, 8, 9	23	2, 3, 5, 6, 8, 10	24	0, 2, 3, 6, 7, 10	25	0, 3, 4, 5, 7, 9
26	0, 1, 3, 4, 5, 7, 9, 10	27	1, 2, 3, 4, 7, 9	28	1, 2, 3, 4, 5, 10	29	0, 4, 6, 8, 9, 10	30	0, 1, 3, 5, 7, 8
31	1, 5, 6, 7, 9, 10	32	0, 7, 9, 10	33	3, 4, 7, 8	34	0, 1, 3, 6, 8, 10	35	3, 6, 9, 10
36	1, 2, 4, 5, 6, 8, 9, 10	37	1, 2, 3, 5, 8, 9	38	0, 2, 3, 5, 8, 9	39	2, 4, 8, 9	40	0, 1, 3, 5
41	0, 5, 6, 9	42	1, 4, 5, 8	43	2, 3, 4, 5, 7, 10	44	1, 2, 3, 4, 5, 6, 7, 10	45	4, 8
46	1, 4, 5, 6, 9, 10	47	4, 5, 6, 10	48	0, 1, 3, 4, 6, 9	49	2, 4, 5, 9	50	0, 3, 6, 7, 8, 10
51	0, 1, 2, 5, 6, 7, 8, 10	52	0, 2, 3, 6, 7, 8, 9, 10	53	1, 2, 3, 4, 5, 7, 8, 9	54	2, 3, 4, 6, 7, 8	55	0, 1, 2, 4, 6, 7
56	2, 4, 6, 8, 9, 10	57	5, 6, 7, 8	58	0, 1, 5, 7, 8, 9	59	0, 1, 2, 3, 4, 6	60	0, 2, 3, 5, 6, 10
61	3, 4, 6, 7, 8, 9	62	1, 2, 3, 7, 9, 10	63	0, 2, 6, 8	64	0, 3, 7, 9	65	0, 1, 3, 5, 8, 10
66	3, 5, 6, 8	67	1, 3, 4, 7	68	0, 1, 2, 5, 6, 9	69	6, 8	70	1, 6, 7, 9
71	1, 3, 5, 6	72	1, 2, 4, 5, 7, 8, 9, 10	73	0, 1, 2, 3, 5, 6, 8, 10	74	2, 4, 5, 6, 7, 10	75	1, 2, 7, 8
76	0, 4, 5, 6, 7, 10	77	0, 2, 3, 6, 7, 8	78	4, 5, 7, 8	79	0, 1, 4, 8, 9, 10	80	0, 2, 6, 10
81	7, 8	82	0, 1, 7, 10	83	0, 1, 4, 5, 7, 8, 9, 10	84	2, 5, 8, 10	85	0, 2, 4, 5, 7, 8
86	3, 4, 6, 8, 9, 10	87	2, 8	88	1, 2, 3, 4, 6, 8, 9, 10	89	1, 2, 4, 5, 6, 8	90	5, 8
91	1, 5, 6, 7, 8, 10	92	1, 2, 7, 8, 9, 10	93	0, 1, 2, 3, 4, 5, 6, 7, 9, 10	94	1, 8, 9, 10	95	1, 5, 8, 10
96	0, 1, 2, 6, 7, 8	97	1, 2, 5, 8	98	4, 7, 8, 10	99	3, 4, 5, 6, 7, 8	100	0, 1, 3, 5, 6, 9
101	2, 5, 7, 8	102	0, 1, 2, 3, 4, 5, 9, 10	103	0, 1, 6, 8	104	0, 1, 3, 4, 5, 6, 7, 9	105	0, 2, 4, 6, 8, 9
106	2, 3, 4, 5, 6, 7, 8, 10	107	2, 3, 4, 5, 9, 10	108	1, 3, 4, 5, 6, 8	109	2, 6, 7, 8	110	0, 1, 2, 3, 4, 8
111	0, 1, 2, 3, 5, 7, 9, 10	112	1, 4, 5, 7, 8, 9	113	3, 4, 5, 8	114	1, 3, 5, 10	115	0, 2, 3, 4, 5, 6, 9, 10
116	0, 2, 3, 5, 7, 10	117	0, 3, 4, 7, 8, 10	118	0, 1, 2, 4, 6, 8	119	0, 1, 2, 4, 6, 7, 8, 9	120	0, 1, 4, 6, 9, 10

(continued)

Table 9.7 (continued)c

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
121	0, 1, 2, 7, 9, 10	122	1, 3, 5, 6, 7, 8	123	0, 2, 4, 5, 8, 9	124	2, 3, 4, 6, 7, 9	125	4, 6, 7, 8
126	0, 1, 4, 5	127	0, 3, 5, 7, 8, 9	128	0, 3, 6, 7	129	1, 2, 3, 5, 6, 7, 9, 10	130	0, 2, 5, 6, 9, 10
131	0, 2, 5, 6, 8, 10	132	1, 5, 6, 10	133	0, 2, 8, 9	134	2, 3, 6, 8	135	1, 2, 5, 9
136	0, 1, 2, 4, 7, 10	137	0, 1, 2, 3, 4, 7, 9, 10	138	1, 5	139	1, 2, 3, 6, 7, 9	140	1, 2, 3, 7
141	0, 1, 3, 6, 8, 9	142	1, 2, 6, 10	143	0, 3, 4, 5, 7, 8	144	2, 3, 4, 5, 7, 8, 9, 10	145	0, 3, 4, 5, 6, 7, 8, 10
146	0, 1, 2, 4, 5, 6, 9, 10	147	0, 1, 3, 4, 5, 10	148	1, 3, 4, 8, 9, 10	149	1, 3, 5, 6, 7, 10	150	2, 3, 4, 5
151	2, 4, 5, 6, 8, 9	152	0, 1, 3, 8, 9, 10	153	0, 2, 3, 7, 8, 10	154	0, 1, 3, 4, 5, 6	155	0, 4, 6, 7, 9, 10
156	3, 5, 8, 10	157	0, 4, 6, 8	158	0, 2, 5, 7, 8, 9	159	0, 2, 3, 5	160	0, 1, 4, 9
161	2, 3, 6, 8, 9, 10	162	3, 5	163	3, 4, 6, 9	164	0, 2, 3, 9	165	1, 2, 4, 5, 6, 7, 9, 10
166	0, 2, 3, 5, 7, 8, 9, 10	167	1, 2, 3, 4, 7, 10	168	4, 5, 9, 10	169	1, 2, 3, 4, 7, 8	170	0, 3, 4, 5, 8, 10
171	1, 2, 4, 5	172	1, 5, 6, 7, 8, 9	173	3, 7, 8, 10	174	4, 5	175	4, 7, 8, 9
176	1, 2, 4, 5, 6, 7, 8, 9	177	2, 5, 7, 10	178	1, 2, 4, 5, 8, 10	179	0, 1, 3, 5, 6, 7	180	5, 10
181	0, 1, 3, 5, 6, 7, 9, 10	182	1, 2, 3, 5, 9, 10	183	2, 5	184	2, 3, 4, 5, 7, 9	185	4, 5, 6, 7, 9, 10
186	0, 1, 2, 3, 4, 6, 7, 8, 9, 10	187	5, 6, 7, 9	188	2, 5, 7, 9	189	3, 4, 5, 8, 9, 10	190	2, 5, 9, 10
191	1, 4, 5, 7	192	0, 1, 2, 3, 4, 5	193	0, 2, 3, 6, 8, 9	194	2, 4, 5, 10	195	0, 1, 2, 6, 7, 8, 9, 10
196	3, 5, 8, 9	197	0, 1, 2, 3, 4, 6, 8, 9	198	1, 3, 5, 6, 8, 10	199	0, 1, 2, 3, 4, 5, 7, 10	200	0, 1, 2, 6, 7, 10
201	0, 1, 2, 3, 5, 9	202	3, 4, 5, 10	203	0, 1, 5, 8, 9, 10	204	0, 2, 4, 6, 7, 8, 9, 10	205	1, 2, 4, 5, 6, 9
206	0, 1, 2, 5	207	0, 2, 7, 9	208	0, 1, 2, 3, 6, 7, 8, 10	209	0, 2, 4, 7, 8, 10	210	0, 1, 4, 5, 7, 8
211	1, 3, 5, 8, 9, 10	212	1, 3, 4, 5, 6, 8, 9, 10	213	1, 3, 6, 7, 8, 9	214	4, 6, 7, 8, 9, 10	215	0, 2, 3, 4, 5, 9
216	1, 2, 5, 6, 8, 10	217	0, 1, 3, 4, 6, 10	218	1, 3, 4, 5	219	1, 2, 8, 9	220	0, 2, 4, 5, 6, 8
221	0, 3, 4, 8	222	0, 2, 3, 4, 6, 7, 9, 10	223	2, 3, 6, 7, 8, 10	224	2, 3, 5, 7, 8, 10	225	2, 3, 7, 9
226	5, 6, 8, 10	227	0, 3, 5, 10	228	2, 6, 9, 10	229	1, 4, 7, 8, 9, 10	230	0, 1, 4, 6, 7, 8, 9, 10
231	2, 9	232	0, 3, 4, 6, 9, 10	233	0, 4, 9, 10	234	0, 3, 5, 6, 8, 9	235	3, 7, 9, 10
236	0, 1, 2, 4, 5, 8	237	0, 1, 2, 4, 5, 6, 7, 10	238	0, 1, 2, 3, 4, 5, 7, 8	239	1, 2, 3, 6, 7, 8, 9, 10	240	0, 1, 2, 7, 8, 9

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
241	0, 1, 5, 6, 7, 9	242	0, 2, 3, 4, 7, 9	243	0, 1, 2, 10	244	1, 2, 3, 5, 6, 10	245	0, 5, 6, 7, 8, 9
246	0, 4, 5, 7, 8, 10	247	0, 1, 2, 3, 8, 9	248	1, 3, 4, 6, 7, 8	249	0, 2, 5, 7	250	1, 3, 5, 8
251	2, 4, 5, 6, 8, 10	252	0, 2, 8, 10	253	1, 6, 8, 9	254	0, 3, 5, 6, 7, 10	255	0, 2
256	0, 1, 3, 6	257	0, 6, 8, 10	258	1, 2, 3, 4, 6, 7, 9, 10	259	0, 2, 4, 5, 6, 7, 8, 10	260	0, 1, 4, 7, 9, 10
261	1, 2, 6, 7	262	0, 1, 4, 5, 9, 10	263	0, 1, 2, 5, 7, 8	264	1, 2, 9, 10	265	2, 3, 4, 5, 6, 9
266	0, 4, 5, 7	267	1, 2	268	1, 4, 5, 6	269	1, 2, 3, 4, 5, 6, 9, 10	270	2, 4, 7, 10
271	1, 2, 5, 7, 9, 10	272	0, 2, 3, 4, 8, 9	273	2, 7	274	0, 2, 3, 4, 6, 7, 8, 9	275	0, 2, 6, 7, 9, 10
276	2, 10	277	0, 1, 2, 4, 6, 10	278	1, 2, 3, 4, 6, 7	279	0, 1, 3, 4, 5, 6, 7, 8, 9, 10	280	2, 3, 4, 6
281	2, 4, 6, 10	282	0, 1, 2, 5, 6, 7	283	2, 6, 7, 10	284	1, 2, 4, 9	285	0, 1, 2, 8, 9, 10
286	0, 3, 5, 6, 8, 10	287	1, 2, 7, 10	288	3, 4, 5, 6, 7, 8, 9, 10	289	0, 2, 5, 6	290	0, 1, 3, 5, 6, 8, 9, 10
291	0, 2, 3, 5, 7, 9	292	0, 1, 2, 4, 7, 8, 9, 10	293	3, 4, 7, 8, 9, 10	294	0, 2, 6, 8, 9, 10	295	0, 1, 2, 7
296	2, 5, 6, 7, 8, 9	297	1, 3, 4, 5, 6, 7, 8, 10	298	1, 2, 3, 6, 9, 10	299	2, 8, 9, 10	300	4, 6, 8, 10
301	0, 3, 4, 5, 7, 8, 9, 10	302	1, 4, 5, 7, 8, 10	303	1, 2, 4, 5, 8, 9	304	0, 2, 5, 6, 7, 9	305	0, 1, 2, 3, 5, 6, 7, 9
306	0, 3, 4, 5, 6, 9	307	1, 3, 4, 5, 6, 7	308	0, 1, 2, 6, 8, 10	309	2, 3, 5, 7, 9, 10	310	0, 1, 3, 7, 8, 9
311	0, 1, 2, 9	312	5, 6, 9, 10	313	1, 2, 3, 5, 8, 10	314	0, 1, 5, 8	315	0, 1, 3, 4, 6, 7, 8, 10
316	0, 3, 4, 5, 7, 10	317	0, 2, 4, 5, 7, 10	318	0, 4, 6, 10	319	2, 3, 5, 7	320	0, 2, 7, 8
321	3, 6, 7, 10	322	1, 4, 5, 6, 7, 9	323	1, 3, 4, 5, 6, 7, 8, 9	324	6, 10	325	0, 1, 3, 6, 7, 8
326	1, 6, 7, 8	327	0, 2, 3, 5, 6, 8	328	0, 4, 6, 7	329	1, 2, 5, 8, 9, 10	330	1, 2, 3, 4, 7, 8, 9, 10
331	0, 1, 2, 4, 5, 8, 9, 10	332	0, 3, 4, 5, 6, 7, 9, 10	333	4, 5, 6, 8, 9, 10	334	2, 3, 4, 6, 8, 9	335	0, 1, 4, 6, 8, 10
336	7, 8, 9, 10	337	0, 2, 3, 7, 9, 10	338	2, 3, 4, 5, 6, 8	339	1, 2, 4, 5, 7, 8	340	0, 5, 6, 8, 9, 10
341	0, 1, 3, 4, 5, 9	342	2, 4, 8, 10	343	0, 2, 5, 9	344	1, 2, 3, 5, 7, 10	345	5, 7, 8, 10
346	3, 5, 6, 9	347	0, 2, 3, 4, 7, 8	348	8, 10	349	0, 3, 8, 9	350	3, 5, 7, 8
351	0, 1, 3, 4, 6, 7, 9, 10	352	1, 2, 3, 4, 5, 7, 8, 10	353	1, 4, 6, 7, 8, 9	354	3, 4, 9, 10	355	1, 2, 6, 7, 8, 9
356	2, 4, 5, 8, 9, 10	357	6, 7, 9, 10	358	0, 1, 2, 3, 6, 10	359	1, 2, 4, 8	360	9, 10

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
361	1, 2, 3, 9	362	0, 1, 2, 3, 6, 7, 9, 10	363	1, 4, 7, 10	364	2, 4, 6, 7, 9, 10	365	0, 1, 5, 6, 8, 10
366	4, 10	367	0, 1, 3, 4, 5, 6, 8, 10	368	3, 4, 6, 7, 8, 10	369	7, 10	370	1, 3, 7, 8, 9, 10
371	0, 1, 3, 4, 9, 10	372	0, 1, 2, 3, 4, 5, 6, 7, 8, 9	373	0, 1, 3, 10	374	1, 3, 7, 10	375	2, 3, 4, 8, 9, 10
376	3, 4, 7, 10	377	1, 6, 9, 10	378	5, 6, 7, 8, 9, 10	379	0, 2, 3, 5, 7, 8	380	4, 7, 9, 10
381	0, 1, 2, 3, 4, 5, 6, 7	382	2, 3, 8, 10	383	0, 2, 3, 5, 6, 7, 8, 9	384	0, 2, 4, 6, 8, 10	385	1, 4, 5, 6, 7, 8, 9, 10
386	0, 1, 4, 5, 6, 7	387	3, 5, 6, 7, 8, 10	388	4, 8, 9, 10	389	2, 3, 4, 5, 6, 10	390	0, 1, 2, 3, 4, 5, 7, 9
391	0, 3, 6, 7, 9, 10	392	5, 6, 7, 10	393	1, 3, 5, 7	394	0, 1, 2, 4, 5, 6, 7, 8	395	1, 2, 4, 5, 7, 9
396	1, 2, 5, 6, 9, 10	397	2, 3, 4, 6, 8, 10	398	0, 2, 3, 4, 6, 8, 9, 10	399	0, 1, 2, 3, 6, 8	400	0, 1, 2, 3, 4, 9
401	3, 5, 7, 8, 9, 10	402	0, 2, 4, 6, 7, 10	403	0, 4, 5, 6, 8, 9	404	6, 8, 9, 10	405	2, 3, 6, 7
406	0, 2, 5, 7, 9, 10	407	2, 5, 8, 9	408	0, 1, 3, 4, 5, 7, 8, 9	409	0, 1, 2, 4, 7, 8	410	1, 2, 4, 7, 8, 10
411	1, 3, 7, 8	412	0, 2, 4, 10	413	4, 5, 8, 10	414	0, 3, 4, 7	415	1, 2, 3, 4, 6, 9
416	0, 1, 2, 3, 4, 5, 6, 9	417	3, 7	418	0, 3, 4, 5, 8, 9	419	3, 4, 5, 9	420	0, 2, 3, 5, 8, 10
421	1, 3, 4, 8	422	2, 5, 6, 7, 9, 10	423	0, 1, 4, 5, 6, 7, 9, 10	424	1, 2, 5, 6, 7, 8, 9, 10	425	0, 1, 2, 3, 4, 6, 7, 8
426	1, 2, 3, 5, 6, 7	427	0, 1, 3, 5, 6, 10	428	1, 3, 5, 7, 8, 9	429	4, 5, 6, 7	430	0, 4, 6, 7, 8, 10
431	0, 1, 2, 3, 5, 10	432	1, 2, 4, 5, 9, 10	433	2, 3, 5, 6, 7, 8	434	0, 1, 2, 6, 8, 9	435	1, 5, 7, 10
436	2, 6, 8, 10	437	0, 2, 4, 7, 9, 10	438	2, 4, 5, 7	439	0, 2, 3, 6	440	0, 1, 4, 5, 8, 10
441	5, 7	442	0, 5, 6, 8	443	0, 2, 4, 5	444	0, 1, 3, 4, 6, 7, 8, 9	445	0, 1, 2, 4, 5, 7, 9, 10
446	1, 3, 4, 5, 6, 9	447	0, 1, 6, 7	448	3, 4, 5, 6, 9, 10	449	1, 2, 5, 6, 7, 10	450	3, 4, 6, 7
451	0, 3, 7, 8, 9, 10	452	1, 5, 9, 10	453	6, 7	454	0, 6, 9, 10	455	0, 3, 4, 6, 7, 8, 9, 10
456	1, 4, 7, 9	457	1, 3, 4, 6, 7, 10	458	2, 3, 5, 7, 8, 9	459	1, 7	460	0, 1, 2, 3, 5, 7, 8, 9
461	0, 1, 3, 4, 5, 7	462	4, 7	463	0, 4, 5, 6, 7, 9	464	0, 1, 6, 7, 8, 9	465	0, 1, 2, 3, 4, 5, 6, 8, 9, 10
466	0, 7, 8, 9	467	0, 4, 7, 9	468	0, 1, 5, 6, 7, 10	469	0, 1, 4, 7	470	3, 6, 7, 9
471	2, 3, 4, 5, 6, 7	472	0, 2, 4, 5, 8, 10	473	1, 4, 6, 7	474	0, 1, 2, 3, 4, 8, 9, 10	475	0, 5, 7, 10
476	0, 2, 3, 4, 5, 6, 8, 10	477	1, 3, 5, 7, 8, 10	478	1, 2, 3, 4, 5, 6, 7, 9	479	1, 2, 3, 4, 8, 9	480	0, 2, 3, 4, 5, 7

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
481	1, 5, 6, 7	482	0, 1, 2, 3, 7, 10	483	0, 1, 2, 4, 6, 8, 9, 10	484	0, 3, 4, 6, 7, 8	485	2, 3, 4, 7
486	0, 2, 4, 9	487	1, 2, 3, 4, 5, 8, 9, 10	488	1, 2, 4, 6, 9, 10	489	2, 3, 6, 7, 9, 10	490	0, 1, 3, 5, 7, 10
491	0, 1, 3, 5, 6, 7, 8, 10	492	0, 3, 5, 8, 9, 10	493	0, 1, 6, 8, 9, 10	494	0, 2, 4, 5, 6, 7	495	1, 3, 4, 7, 8, 10
496	1, 2, 3, 5, 6, 8	497	3, 5, 6, 7	498	0, 3, 4, 10	499	2, 4, 6, 7, 8, 10	500	2, 5, 6, 10
501	0, 1, 2, 4, 5, 6, 8, 9	502	1, 4, 5, 8, 9, 10	503	1, 4, 5, 7, 9, 10	504	0, 4, 5, 9	505	1, 7, 8, 10
506	1, 2, 5, 7	507	0, 1, 4, 8	508	0, 1, 3, 6, 9, 10	509	0, 1, 2, 3, 6, 8, 9, 10	510	0, 4
511	0, 1, 2, 5, 6, 8	512	0, 1, 2, 6	513	0, 2, 5, 7, 8, 10	514	0, 1, 5, 9	515	2, 3, 4, 6, 7, 10
516	1, 2, 3, 4, 6, 7, 8, 9	517	2, 3, 4, 5, 6, 7, 9, 10	518	0, 1, 3, 4, 5, 8, 9, 10	519	0, 2, 3, 4, 9, 10	520	0, 2, 3, 7, 8, 9
521	0, 2, 4, 5, 6, 9	522	1, 2, 3, 4	523	1, 3, 4, 5, 7, 8	524	0, 2, 7, 8, 9, 10	525	1, 2, 6, 7, 9, 10
526	0, 2, 3, 4, 5, 10	527	3, 5, 6, 8, 9, 10	528	2, 4, 7, 9	529	3, 5, 7, 10	530	1, 4, 6, 7, 8, 10
531	1, 2, 4, 10	532	0, 3, 8, 10	533	1, 2, 5, 7, 8, 9	534	2, 4	535	2, 3, 5, 8
536	1, 2, 8, 10	537	0, 1, 3, 4, 5, 6, 8, 9	538	1, 2, 4, 6, 7, 8, 9, 10	539	0, 1, 2, 3, 6, 9	540	3, 4, 8, 9
541	0, 1, 2, 3, 6, 7	542	2, 3, 4, 7, 9, 10	543	0, 1, 3, 4	544	0, 4, 5, 6, 7, 8	545	2, 6, 7, 9
546	3, 4	547	3, 6, 7, 8	548	0, 1, 3, 4, 5, 6, 7, 8	549	1, 4, 6, 9	550	0, 1, 3, 4, 7, 9
551	0, 2, 4, 5, 6, 10	552	4, 9	553	0, 2, 4, 5, 6, 8, 9, 10	554	0, 1, 2, 4, 8, 9	555	1, 4
556	1, 2, 3, 4, 6, 8	557	3, 4, 5, 6, 8, 9	558	0, 1, 2, 3, 5, 6, 7, 8, 9, 10	559	4, 5, 6, 8	560	1, 4, 6, 8
561	2, 3, 4, 7, 8, 9	562	1, 4, 8, 9	563	0, 3, 4, 6	564	0, 1, 2, 3, 4, 10	565	1, 2, 5, 7, 8, 10
566	1, 3, 4, 9	567	0, 1, 5, 6, 7, 8, 9, 10	568	2, 4, 7, 8	569	0, 1, 2, 3, 5, 7, 8, 10	570	0, 2, 4, 5, 7, 9
571	0, 1, 2, 3, 4, 6, 9, 10	572	0, 1, 5, 6, 9, 10	573	0, 1, 2, 4, 8, 10	574	2, 3, 4, 9	575	0, 4, 7, 8, 9, 10
576	1, 3, 5, 6, 7, 8, 9, 10	577	0, 1, 3, 4, 5, 8	578	0, 1, 4, 10	579	1, 6, 8, 10	580	0, 1, 2, 5, 6, 7, 9, 10
581	1, 3, 6, 7, 9, 10	582	0, 3, 4, 6, 7, 10	583	0, 2, 4, 7, 8, 9	584	0, 2, 3, 4, 5, 7, 8, 9	585	0, 2, 5, 6, 7, 8
586	3, 5, 6, 7, 8, 9	587	1, 2, 3, 4, 8, 10	588	0, 1, 4, 5, 7, 9	589	0, 2, 3, 5, 9, 10	590	0, 2, 3, 4
591	0, 1, 7, 8	592	1, 3, 4, 5, 7, 10	593	2, 3, 7, 10	594	1, 2, 3, 5, 6, 8, 9, 10	595	1, 2, 5, 6, 7, 9

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
596	1, 2, 4, 6, 7, 9	597	1, 2, 6, 8	598	4, 5, 7, 9	599	2, 4, 9, 10	600	1, 5, 8, 9
601	0, 3, 6, 7, 8, 9	602	0, 3, 5, 6, 7, 8, 9, 10	603	1, 8	604	2, 3, 5, 8, 9, 10	605	3, 8, 9, 10
606	2, 4, 5, 7, 8, 10	607	2, 6, 8, 9	608	0, 1, 3, 4, 7, 10	609	0, 1, 3, 4, 5, 6, 9, 10	610	0, 1, 2, 3, 4, 6, 7, 10
611	0, 1, 2, 5, 6, 7, 8, 9	612	0, 1, 6, 7, 8, 10	613	0, 4, 5, 6, 8, 10	614	1, 2, 3, 6, 8, 10	615	0, 1, 9, 10
616	0, 1, 2, 4, 5, 9	617	4, 5, 6, 7, 8, 10	618	3, 4, 6, 7, 9, 10	619	0, 1, 2, 7, 8, 10	620	0, 2, 3, 5, 6, 7
621	1, 4, 6, 10	622	0, 2, 4, 7	623	1, 3, 4, 5, 7, 9	624	1, 7, 9, 10	625	0, 5, 7, 8
626	2, 4, 5, 6, 9, 10	627	1, 10	628	0, 2, 5, 10	629	5, 7, 9, 10	630	0, 1, 2, 3, 5, 6, 8, 9
631	1, 3, 4, 5, 6, 7, 9, 10	632	0, 3, 6, 8, 9, 10	633	0, 1, 5, 6	634	0, 3, 4, 8, 9, 10	635	0, 1, 4, 6, 7, 10
636	0, 1, 8, 9	637	1, 2, 3, 4, 5, 8	638	3, 4, 6, 10	639	0, 1	640	0, 3, 4, 5
641	0, 1, 2, 3, 4, 5, 8, 9	642	1, 3, 6, 9	643	0, 1, 4, 6, 8, 9	644	1, 2, 3, 7, 8, 10	645	1, 6
646	1, 2, 3, 5, 6, 7, 8, 10	647	1, 5, 6, 8, 9, 10	648	1, 9	649	0, 1, 3, 5, 9, 10	650	0, 1, 2, 3, 5, 6
651	0, 2, 3, 4, 5, 6, 7, 8, 9, 10	652	1, 2, 3, 5	653	1, 3, 5, 9	654	0, 1, 4, 5, 6, 10	655	1, 5, 6, 9
656	0, 1, 3, 8	657	0, 1, 7, 8, 9, 10	658	2, 4, 5, 7, 9, 10	659	0, 1, 6, 9	660	2, 3, 4, 5, 6, 7, 8, 9
661	1, 4, 5, 10	662	0, 2, 4, 5, 7, 8, 9, 10	663	1, 2, 4, 6, 8, 10	664	0, 1, 3, 6, 7, 8, 9, 10	665	2, 3, 6, 7, 8, 9
666	1, 5, 7, 8, 9, 10	667	0, 1, 6, 10	668	1, 4, 5, 6, 7, 8	669	0, 2, 3, 4, 5, 6, 7, 9	670	0, 1, 2, 5, 8, 9
671	1, 7, 8, 9	672	3, 5, 7, 9	673	2, 3, 4, 6, 7, 8, 9, 10	674	0, 3, 4, 6, 7, 9	675	0, 1, 3, 4, 7, 8
676	1, 4, 5, 6, 8, 10	677	0, 1, 2, 4, 5, 6, 8, 10	678	2, 3, 4, 5, 8, 10	679	0, 2, 3, 4, 5, 6	680	0, 1, 5, 7, 9, 10
681	1, 2, 4, 6, 8, 9	682	0, 2, 6, 7, 8, 10	683	0, 1, 8, 10	684	4, 5, 8, 9	685	0, 1, 2, 4, 7, 9
686	0, 4, 7, 10	687	0, 2, 3, 5, 6, 7, 9, 10	688	2, 3, 4, 6, 9, 10	689	1, 3, 4, 6, 9, 10	690	3, 5, 9, 10
691	1, 2, 4, 6	692	1, 6, 7, 10	693	2, 5, 6, 9	694	0, 3, 4, 5, 6, 8	695	0, 2, 3, 4, 5, 6, 7, 8
696	5, 9	697	0, 2, 5, 6, 7, 10	698	0, 5, 6, 7	699	1, 2, 4, 5, 7, 10	700	3, 5, 6, 10
701	0, 1, 4, 7, 8, 9	702	0, 1, 2, 3, 6, 7, 8, 9	703	0, 1, 3, 4, 7, 8, 9, 10	704	2, 3, 4, 5, 6, 8, 9, 10	705	3, 4, 5, 7, 8, 9
706	1, 2, 3, 5, 7, 8	707	0, 3, 5, 7, 9, 10	708	6, 7, 8, 9	709	1, 2, 6, 8, 9, 10	710	1, 2, 3, 4, 5, 7

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
711	0, 1, 3, 4, 6, 7	712	4, 5, 7, 8, 9, 10	713	0, 2, 3, 4, 8, 10	714	1, 3, 7, 9	715	1, 4, 8, 10
716	0, 1, 2, 4, 6, 9	717	4, 6, 7, 9	718	2, 4, 5, 8	719	1, 2, 3, 6, 7, 10	720	7, 9
721	2, 7, 8, 10	722	2, 4, 6, 7	723	0, 2, 3, 5, 6, 8, 9, 10	724	0, 1, 2, 3, 4, 6, 7, 9	725	0, 3, 5, 6, 7, 8
726	2, 3, 8, 9	727	0, 1, 5, 6, 7, 8	728	1, 3, 4, 7, 8, 9	729	5, 6, 8, 9	730	0, 1, 2, 5, 9, 10
731	0, 1, 3, 7	732	8, 9	733	0, 1, 2, 8	734	0, 1, 2, 5, 6, 8, 9, 10	735	0, 3, 6, 9
736	1, 3, 5, 6, 8, 9	737	0, 4, 5, 7, 9, 10	738	3, 9	739	0, 2, 3, 4, 5, 7, 9, 10	740	2, 3, 5, 6, 7, 9
741	6, 9	742	0, 2, 6, 7, 8, 9	743	0, 2, 3, 8, 9, 10	744	0, 1, 2, 3, 4, 5, 6, 7, 8, 10	745	0, 2, 9, 10
746	0, 2, 6, 9	747	1, 2, 3, 7, 8, 9	748	2, 3, 6, 9	749	0, 5, 8, 9	750	4, 5, 6, 7, 8, 9
751	1, 2, 4, 6, 7, 10	752	3, 6, 8, 9	753	0, 1, 2, 3, 4, 5, 6, 10	754	1, 2, 7, 9	755	1, 2, 4, 5, 6, 7, 8, 10
756	1, 3, 5, 7, 9, 10	757	0, 3, 4, 5, 6, 7, 8, 9	758	0, 3, 4, 5, 6, 10	759	2, 4, 5, 6, 7, 9	760	3, 7, 8, 9
761	1, 2, 3, 4, 5, 9	762	0, 1, 2, 3, 4, 6, 8, 10	763	2, 5, 6, 8, 9, 10	764	4, 5, 6, 9	765	0, 2, 4, 6
766	0, 1, 3, 4, 5, 6, 7, 10	767	0, 1, 3, 4, 6, 8	768	0, 1, 4, 5, 8, 9	769	1, 2, 3, 5, 7, 9	770	1, 2, 3, 5, 7, 8, 9, 10
771	0, 1, 2, 5, 7, 10	772	0, 1, 2, 3, 8, 10	773	2, 4, 6, 7, 8, 9	774	1, 3, 5, 6, 9, 10	775	3, 4, 5, 7, 8, 10
776	5, 7, 8, 9	777	1, 2, 5, 6	778	1, 4, 6, 8, 9, 10	779	1, 4, 7, 8	780	0, 2, 3, 4, 6, 7, 8, 10
781	0, 1, 3, 6, 7, 10	782	0, 1, 3, 6, 7, 9	783	0, 2, 6, 7	784	1, 3, 9, 10	785	3, 4, 7, 9
786	2, 3, 6, 10	787	0, 1, 2, 3, 5, 8	788	0, 1, 2, 3, 4, 5, 8, 10	789	2, 6	790	2, 3, 4, 7, 8, 10
791	2, 3, 4, 8	792	1, 2, 4, 7, 9, 10	793	0, 2, 3, 7	794	1, 4, 5, 6, 8, 9	795	0, 3, 4, 5, 6, 8, 9, 10
796	0, 1, 4, 5, 6, 7, 8, 9	797	0, 1, 2, 3, 5, 6, 7, 10	798	0, 1, 2, 4, 5, 6	799	0, 2, 4, 5, 9, 10	800	0, 2, 4, 6, 7, 8
801	3, 4, 5, 6	802	3, 5, 6, 7, 9, 10	803	0, 1, 2, 4, 9, 10	804	0, 1, 3, 4, 8, 9	805	1, 2, 4, 5, 6, 7
806	0, 1, 5, 7, 8, 10	807	0, 4, 6, 9	808	1, 5, 7, 9	809	1, 3, 6, 8, 9, 10	810	1, 3, 4, 6
811	1, 2, 5, 10	812	0, 3, 4, 7, 9, 10	813	4, 6	814	4, 5, 7, 10	815	1, 3, 4, 10
816	0, 2, 3, 5, 6, 7, 8, 10	817	0, 1, 3, 4, 6, 8, 9, 10	818	0, 2, 3, 4, 5, 8	819	0, 5, 6, 10	820	2, 3, 4, 5, 8, 9
821	0, 1, 4, 5, 6, 9	822	2, 3, 5, 6	823	2, 6, 7, 8, 9, 10	824	0, 4, 8, 9	825	5, 6
826	5, 8, 9, 10	827	2, 3, 5, 6, 7, 8, 9, 10	828	0, 3, 6, 8	829	0, 2, 3, 5, 6, 9	830	1, 2, 4, 6, 7, 8
831	0, 6	832	0, 1, 2, 4, 6, 7, 8, 10	833	0, 2, 3, 4, 6, 10	834	3, 6	835	3, 4, 5, 6, 8, 10

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
836	0, 5, 6, 7, 8, 10	837	0, 1, 2, 3, 4, 5, 7, 8, 9, 10	838	6, 7, 8, 10	839	3, 6, 8, 10	840	0, 4, 5, 6, 9, 10
841	0, 3, 6, 10	842	2, 5, 6, 8	843	1, 2, 3, 4, 5, 6	844	1, 3, 4, 7, 9, 10	845	0, 3, 5, 6
846	0, 1, 2, 3, 7, 8, 9, 10	847	4, 6, 9, 10	848	1, 2, 3, 4, 5, 7, 9, 10	849	0, 2, 4, 6, 7, 9	850	0, 1, 2, 3, 4, 5, 6, 8
851	0, 1, 2, 3, 7, 8	852	1, 2, 3, 4, 6, 10	853	0, 4, 5, 6	854	0, 1, 2, 6, 9, 10	855	0, 1, 3, 5, 7, 8, 9, 10
856	2, 3, 5, 6, 7, 10	857	1, 2, 3, 6	858	1, 3, 8, 10	859	0, 1, 2, 3, 4, 7, 8, 9	860	0, 1, 3, 5, 8, 9
861	1, 2, 5, 6, 8, 9	862	0, 2, 4, 6, 9, 10	863	0, 2, 4, 5, 6, 7, 9, 10	864	2, 4, 7, 8, 9, 10	865	0, 5, 7, 8, 9, 10
866	1, 3, 4, 5, 6, 10	867	0, 2, 3, 6, 7, 9	868	0, 1, 2, 4, 5, 7	869	2, 4, 5, 6	870	2, 3, 9, 10
871	1, 3, 5, 6, 7, 9	872	1, 4, 5, 9	873	0, 1, 3, 4, 5, 7, 8, 10	874	0, 3, 4, 7, 8, 9	875	0, 3, 4, 6, 8, 9
876	3, 4, 8, 10	877	0, 6, 7, 9	878	0, 1, 4, 6	879	0, 3, 7, 10	880	0, 2, 5, 8, 9, 10
881	0, 1, 2, 5, 7, 8, 9, 10	882	3, 10	883	0, 1, 4, 5, 7, 10	884	0, 1, 5, 10	885	1, 4, 6, 7, 9, 10
886	0, 4, 8, 10	887	1, 2, 3, 5, 6, 9	888	0, 1, 2, 3, 5, 6, 7, 8	889	1, 2, 3, 4, 5, 6, 8, 9	890	0, 2, 3, 4, 7, 8, 9, 10
891	1, 2, 3, 8, 9, 10	892	1, 2, 6, 7, 8, 10	893	1, 3, 4, 5, 8, 10	894	0, 1, 2, 3	895	0, 2, 3, 4, 6, 7
896	1, 6, 7, 8, 9, 10	897	0, 1, 5, 6, 8, 9	898	1, 2, 3, 4, 9, 10	899	2, 4, 5, 7, 8, 9	900	1, 3, 6, 8
901	2, 4, 6, 9	902	0, 3, 5, 6, 7, 9	903	0, 1, 3, 9	904	2, 7, 9, 10	905	0, 1, 4, 6, 7, 8
906	1, 3	907	1, 2, 4, 7	908	0, 1, 7, 9	909	0, 2, 3, 4, 5, 7, 8, 10	910	0, 1, 3, 5, 6, 7, 8, 9
911	0, 1, 2, 5, 8, 10	912	2, 3, 7, 8	913	0, 1, 2, 5, 6, 10	914	1, 2, 3, 6, 8, 9	915	0, 2, 3, 10
916	3, 4, 5, 6, 7, 10	917	1, 5, 6, 8	918	2, 3	919	2, 5, 6, 7	920	0, 2, 3, 4, 5, 6, 7, 10
921	0, 3, 5, 8	922	0, 2, 3, 6, 8, 10	923	1, 3, 4, 5, 9, 10	924	3, 8	925	1, 3, 4, 5, 7, 8, 9, 10
926	0, 1, 3, 7, 8, 10	927	0, 3	928	0, 1, 2, 3, 5, 7	929	2, 3, 4, 5, 7, 8	930	0, 1, 2, 4, 5, 6, 7, 8, 9, 10
931	3, 4, 5, 7	932	0, 3, 5, 7	933	1, 2, 3, 6, 7, 8	934	0, 3, 7, 8	935	2, 3, 5, 10
936	0, 1, 2, 3, 9, 10	937	0, 1, 4, 6, 7, 9	938	0, 2, 3, 8	939	0, 4, 5, 6, 7, 8, 9, 10	940	1, 3, 6, 7
941	0, 1, 2, 4, 6, 7, 9, 10	942	1, 3, 4, 6, 8, 10	943	0, 1, 2, 3, 5, 8, 9, 10	944	0, 4, 5, 8, 9, 10	945	0, 1, 3, 7, 9, 10
946	1, 2, 3, 8	947	3, 6, 7, 8, 9, 10	948	0, 2, 4, 5, 6, 7, 8, 9	949	0, 2, 3, 4, 7, 10	950	0, 3, 9, 10
951	0, 5, 7, 9	952	0, 1, 4, 5, 6, 8, 9, 10	953	0, 2, 5, 6, 8, 9	954	2, 3, 5, 6, 9, 10	955	1, 3, 6, 7, 8, 10
956	1, 2, 3, 4, 6, 7, 8, 10	957	1, 4, 5, 6, 7, 10	958	2, 4, 5, 6, 7, 8	959	0, 1, 2, 3, 7, 9	960	0, 3, 4, 6, 8, 10

(continued)

Table 9.7 (continued)

i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$	i	$\alpha(x)^i$
961	1, 2, 4, 8, 9, 10	962	1, 2, 3, 10	963	0, 6, 7, 10	964	0, 2, 3, 4, 6, 9	965	1, 2, 6, 9
966	0, 1, 2, 4, 5, 7, 8, 9	967	0, 1, 4, 5, 6, 8	968	0, 1, 3, 5, 6, 8	969	0, 1, 5, 7	970	3, 4, 6, 8
971	1, 3, 8, 9	972	0, 4, 7, 8	973	2, 5, 6, 7, 8, 10	974	2, 4, 5, 6, 7, 8, 9, 10	975	0, 7
976	1, 2, 4, 7, 8, 9	977	2, 7, 8, 9	978	1, 3, 4, 6, 7, 9	979	1, 5, 7, 8	980	0, 2, 3, 6, 9, 10
981	0, 2, 3, 4, 5, 8, 9, 10	982	0, 1, 2, 3, 5, 6, 9, 10	983	0, 1, 4, 5, 6, 7, 8, 10	984	0, 5, 6, 7, 9, 10	985	3, 4, 5, 7, 9, 10
986	0, 1, 2, 5, 7, 9	987	0, 8, 9, 10	988	0, 1, 3, 4, 8, 10	989	3, 4, 5, 6, 7, 9	990	2, 3, 5, 6, 8, 9
991	0, 1, 6, 7, 9, 10	992	1, 2, 4, 5, 6, 10	993	0, 3, 5, 9	994	1, 3, 6, 10	995	0, 2, 3, 4, 6, 8
996	0, 6, 8, 9	997	4, 6, 7, 10	998	1, 3, 4, 5, 8, 9	999	0, 9	1000	1, 4, 9, 10
1001	4, 6, 8, 9	1002	0, 1, 2, 4, 5, 7, 8, 10	1003	0, 2, 3, 4, 5, 6, 8, 9	1004	2, 5, 7, 8, 9, 10	1005	0, 4, 5, 10
1006	2, 3, 7, 8, 9, 10	1007	0, 3, 5, 6, 9, 10	1008	0, 7, 8, 10	1009	0, 1, 2, 3, 4, 7	1010	2, 3, 5, 9
1011	0, 10	1012	2, 3, 4, 10	1013	0, 1, 2, 3, 4, 7, 8, 10	1014	0, 2, 5, 8	1015	0, 3, 5, 7, 8, 10
1016	0, 1, 2, 6, 7, 9	1017	0, 5	1018	0, 1, 2, 4, 5, 6, 7, 9	1019	0, 4, 5, 7, 8, 9	1020	0, 8
1021	0, 2, 4, 8, 9, 10	1022	0, 1, 2, 4, 5, 10	1023	1, 2, 3, 4, 5, 6, 7, 8, 9, 10				

Table 9.8 Circulant analysis $p = 11$, $j(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10}$, factors of $1 + x^p$

i	$j(x)^i$
1	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Weight Distributions of Quadratic Double-Circulant Codes and their Modulo Congruence

Primes +3 Modulo 8

Prime 11

We have $P = \left[\begin{smallmatrix} 1 & 3 \\ 3 & 10 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 10 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(11)$, and the permutations of order 3, 5 and 11 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 10 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 10 & 3 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 10 & 9 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(11) = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot = 660$$

and the weight enumerator polynomials of the invariant subcodes are

$$\begin{aligned}
A^{G_2^0}_{\mathscr{B}_{11}}(z) &= \left(1 + z^{24}\right) + 15 \cdot \left(z^8 + z^{16}\right) + 32 \cdot z^{12} \\
A^{G_4}_{\mathscr{B}_{11}}(z) &= \left(1 + z^{24}\right) + 3 \cdot \left(z^8 + z^{16}\right) + 8 \cdot z^{12} \\
A^{S_3}_{\mathscr{B}_{11}}(z) &= \left(1 + z^{24}\right) + 14 \cdot z^{12} \\
A^{S_5}_{\mathscr{B}_{11}}(z) &= \left(1 + z^{24}\right) + 4 \cdot \left(z^8 + z^{16}\right) + 6 \cdot z^{12} \\
A^{S_{11}}_{\mathscr{B}_{11}}(z) &= \left(1 + z^{24}\right) + 2 \cdot z^{12}\,.
\end{aligned}$$

The weight distributions of $\mathscr{B}_{11}$ and their modular congruence are shown in Table 9.9.

Table 9.9 Modular congruence weight distributions of $\mathscr{B}_{11}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3	$A_i(S_5)$ mod 5	$A_i(S_{11})$ mod 11	$A_i(\mathscr{H})$ mod 660	n_i[a]	A_i
0	1	1	1	1	1	0	1
8	3	0	4	0	99	1	759
12	0	2	1	2	596	3	2576
16	3	0	4	0	99	1	759
24	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{660}$

Prime 19

We have $P = \left[\begin{smallmatrix} 1 & 6 \\ 6 & 18 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 18 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(19)$, and the permutations of order 3, 5 and 19 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 18 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 18 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 18 & 17 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(19) = 2^2 \cdot 3^2 \cdot 5 \cdot 19 \cdot = 3420$$

and the weight enumerator polynomials of the invariant subcodes are

$$A^{(G_2^0)}_{\mathscr{B}_{19}}(z) = \left(1 + z^{40}\right) + 5 \cdot \left(z^8 + z^{32}\right) + 80 \cdot \left(z^{12} + z^{28}\right) + 250 \cdot \left(z^{16} + z^{24}\right) + 352 \cdot z^{20}$$
$$A^{(G_4)}_{\mathscr{B}_{19}}(z) = \left(1 + z^{40}\right) + 1 \cdot \left(z^8 + z^{32}\right) + 8 \cdot \left(z^{12} + z^{28}\right) + 14 \cdot \left(z^{16} + z^{24}\right) + 16 \cdot z^{20}$$
$$A^{(S_3)}_{\mathscr{B}_{19}}(z) = \left(1 + z^{40}\right) + 6 \cdot \left(z^8 + z^{32}\right) + 22 \cdot \left(z^{12} + z^{28}\right) + 57 \cdot \left(z^{16} + z^{24}\right) + 84 \cdot z^{20}$$
$$A^{(S_5)}_{\mathscr{B}_{19}}(z) = \left(1 + z^{40}\right) + 14 \cdot z^{20}$$
$$A^{(S_{19})}_{\mathscr{B}_{19}}(z) = \left(1 + z^{40}\right) + 2 \cdot z^{20}.$$

The weight distributions of $\mathscr{B}_{19}$ and their modular congruence are shown in Table 9.10.

Prime 43

We have $P = \left[\begin{smallmatrix} 1 & 16 \\ 16 & 42 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 42 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(43)$, and the permutations of order 3, 7, 11 and 43 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 42 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 42 & 8 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 42 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 42 & 41 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(43) = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43 \cdot = 39732$$

Table 9.10 Modular congruence weight distributions of $\mathscr{B}_{19}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3^2	$A_i(S_5)$ mod 5	$A_i(S_{19})$ mod 19	$A_i(\mathscr{H})$ mod 3420	n_i[a]	A_i
0	1	1	1	1	1	0	1
8	1	6	0	0	285	0	285
12	0	4	0	0	760	6	21280
16	2	3	0	0	570	70	239970
20	0	3	4	2	2244	153	525504
24	2	3	0	0	570	70	239970
28	0	4	0	0	760	6	21280
32	1	6	0	0	285	0	285
40	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{3420}$

and the weight enumerator polynomials of the invariant subcodes are

$$\begin{aligned}
A^{(G_2^0)}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+44\cdot\left(z^{16}+z^{72}\right)+1232\cdot\left(z^{20}+z^{68}\right)+10241\cdot\left(z^{24}+z^{64}\right)+\\
&\quad 54560\cdot\left(z^{28}+z^{60}\right)+198374\cdot\left(z^{32}+z^{56}\right)+491568\cdot\left(z^{36}+z^{52}\right)+\\
&\quad 839916\cdot\left(z^{40}+z^{48}\right)+1002432\cdot z^{44}\\
A^{(G_4)}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+32\cdot\left(z^{20}+z^{68}\right)+77\cdot\left(z^{24}+z^{64}\right)+160\cdot\left(z^{28}+z^{60}\right)+\\
&\quad 330\cdot\left(z^{32}+z^{56}\right)+480\cdot\left(z^{36}+z^{52}\right)+616\cdot\left(z^{40}+z^{48}\right)+704\cdot z^{44}\\
A^{(S_3)}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+7\cdot\left(z^{16}+z^{72}\right)+168\cdot\left(z^{20}+z^{68}\right)+445\cdot\left(z^{24}+z^{64}\right)+\\
&\quad 1960\cdot\left(z^{28}+z^{60}\right)+4704\cdot\left(z^{32}+z^{56}\right)+7224\cdot\left(z^{36}+z^{52}\right)+\\
&\quad 10843\cdot\left(z^{40}+z^{48}\right)+14832\cdot z^{44}\\
A^{(S_7)}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+6\cdot\left(z^{16}+z^{72}\right)+16\cdot\left(z^{24}+z^{64}\right)+6\cdot\left(z^{28}+z^{60}\right)+\\
&\quad 9\cdot\left(z^{32}+z^{56}\right)+48\cdot\left(z^{36}+z^{52}\right)+84\cdot z^{44}\\
A^{(S_{11})}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+14\cdot z^{44}\\
A^{(S_{43})}_{\mathscr{B}_{43}}(z) &= \left(1+z^{88}\right)+2\cdot z^{44}.
\end{aligned}$$

The weight distributions of $\mathscr{B}_{43}$ and their modular congruence are shown in Table 9.11.

Prime 59

We have $P=\left[\begin{smallmatrix}1 & 23\\ 23 & 58\end{smallmatrix}\right]$ and $T=\left[\begin{smallmatrix}0 & 58\\ 1 & 0\end{smallmatrix}\right]$, $P,T\in \mathrm{PSL}_2(59)$, and the permutations of order 3, 5, 29 and 59 are generated by $\left[\begin{smallmatrix}0 & 1\\ 58 & 1\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0 & 1\\ 58 & 25\end{smallmatrix}\right]$, $\left[\begin{smallmatrix}0 & 1\\ 58 & 3\end{smallmatrix}\right]$ and $\left[\begin{smallmatrix}0 & 1\\ 58 & 57\end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(59)=2^2\cdot 3\cdot 5\cdot 29\cdot 59\cdot=102660$$

and the weight enumerator polynomials of the invariant subcodes are

$$\begin{aligned}
A^{(G_2^0)}_{\mathscr{B}_{59}}(z) &= \left(1+z^{120}\right)+90\cdot\left(z^{20}+z^{100}\right)+2555\cdot\left(z^{24}+z^{96}\right)+\\
&\quad 32700\cdot\left(z^{28}+z^{92}\right)+278865\cdot\left(z^{32}+z^{88}\right)+1721810\cdot\left(z^{36}+z^{84}\right)+\\
&\quad 7807800\cdot\left(z^{40}+z^{80}\right)+26366160\cdot\left(z^{44}+z^{76}\right)+67152520\cdot\left(z^{48}+z^{72}\right)+\\
&\quad 130171860\cdot\left(z^{52}+z^{68}\right)+193193715\cdot\left(z^{56}+z^{64}\right)+220285672\cdot z^{60}
\end{aligned}$$

Table 9.11 Modular congruence weight distributions of $\mathscr{B}_{43}$

i	$A_i(S_2) \bmod 2^2$	$A_i(S_3) \bmod 3$	$A_i(S_7) \bmod 7$	$A_i(S_{11}) \bmod 11$	$A_i(S_{43}) \bmod 43$	$A_i(\mathscr{H}) \bmod 39732$	n_i [a]	A_i
0	1	1	1	1	1	1	0	1
16	0	1	6	0	0	32164	0	32164
20	0	0	0	0	0	0	176	6992832
24	1	1	2	0	0	25069	13483	535731625
28	0	1	6	0	0	32164	418387	16623384448
32	2	0	2	0	0	8514	5673683	225426781470
36	0	0	6	0	0	5676	35376793	1405590745152
40	0	1	0	0	0	26488	104797219	4163803131796
44	0	0	0	3	2	28812	150211729	5968212445440
48	0	1	0	0	0	26488	104797219	4163803131796
52	0	0	6	0	0	5676	35376793	1405590745152
56	2	0	2	0	0	8514	5673683	225426781470
60	0	1	6	0	0	32164	418387	16623384448
64	1	1	2	0	0	25069	13483	535731625
68	0	0	0	0	0	0	176	6992832
72	0	1	6	0	0	32164	0	32164
88	1	1	1	1	1	1	0	1

[a] $n_i = \dfrac{A_i - A_i(\mathscr{H})}{39732}$

$$A^{(G_4)}_{\mathscr{B}_{59}}(z) = \left(1+z^{120}\right) + 6\cdot\left(z^{20}+z^{100}\right) + 19\cdot\left(z^{24}+z^{96}\right) + 132\cdot\left(z^{28}+z^{92}\right) +$$
$$393\cdot\left(z^{32}+z^{88}\right) + 878\cdot\left(z^{36}+z^{84}\right) + 1848\cdot\left(z^{40}+z^{80}\right) + 3312\cdot\left(z^{44}+z^{76}\right) +$$
$$5192\cdot\left(z^{48}+z^{72}\right) + 7308\cdot\left(z^{52}+z^{68}\right) + 8931\cdot\left(z^{56}+z^{64}\right) + 9496\cdot z^{60}$$
$$A^{(S_3)}_{\mathscr{B}_{59}}(z) = \left(1+z^{120}\right) + 285\cdot\left(z^{24}+z^{96}\right) + 21280\cdot\left(z^{36}+z^{84}\right) +$$
$$239970\cdot\left(z^{48}+z^{72}\right) + 525504\cdot z^{60}$$
$$A^{(S_5)}_{\mathscr{B}_{59}}(z) = \left(1+z^{120}\right) + 12\cdot\left(z^{20}+z^{100}\right) + 711\cdot\left(z^{40}+z^{80}\right) + 2648\cdot z^{60}$$
$$A^{(S_{29})}_{\mathscr{B}_{59}}(z) = \left(1+z^{120}\right) + 4\cdot\left(z^{32}+z^{88}\right) + 6\cdot z^{60}$$
$$A^{(S_{59})}_{\mathscr{B}_{59}}(z) = \left(1+z^{120}\right) + 2\cdot z^{60}.$$

The weight distributions of $\mathscr{B}_{59}$ and their modular congruence are shown in Table 9.12.

Prime 67

We have $P = \left[\begin{smallmatrix} 1 & 20 \\ 20 & 66 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 66 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(67)$, and the permutations of order 3, 11, 17 and 67 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 66 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 66 & 17 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 66 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 66 & 65 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(67) = 2^2\cdot 3\cdot 11\cdot 17\cdot 67\cdot = 150348$$

and the weight enumerator polynomials of the invariant subcodes are

$$A^{(G_2^0)}_{\mathscr{B}_{67}}(z) = \left(1+z^{136}\right) + 578\cdot\left(z^{24}+z^{112}\right) + 14688\cdot\left(z^{28}+z^{108}\right) +$$
$$173247\cdot\left(z^{32}+z^{104}\right) + 1480768\cdot\left(z^{36}+z^{100}\right) + 9551297\cdot\left(z^{40}+z^{96}\right) +$$
$$46687712\cdot\left(z^{44}+z^{92}\right) + 175068210\cdot\left(z^{48}+z^{88}\right) + 509510400\cdot\left(z^{52}+z^{84}\right) +$$
$$1160576876\cdot\left(z^{56}+z^{80}\right) + 2081112256\cdot\left(z^{60}+z^{76}\right) + 2949597087\cdot\left(z^{64}+z^{72}\right) +$$
$$3312322944\cdot z^{68}$$
$$A^{(G_4)}_{\mathscr{B}_{67}}(z) = \left(1+z^{136}\right) + 18\cdot\left(z^{24}+z^{112}\right) + 88\cdot\left(z^{28}+z^{108}\right) + 271\cdot\left(z^{32}+z^{104}\right) +$$
$$816\cdot\left(z^{36}+z^{100}\right) + 2001\cdot\left(z^{40}+z^{96}\right) + 4344\cdot\left(z^{44}+z^{92}\right) +$$
$$8386\cdot\left(z^{48}+z^{88}\right) + 14144\cdot\left(z^{52}+z^{84}\right) + 21260\cdot\left(z^{56}+z^{80}\right) +$$
$$28336\cdot\left(z^{60}+z^{76}\right) + 33599\cdot\left(z^{64}+z^{72}\right) + 35616\cdot z^{68}$$
$$A^{(S_3)}_{\mathscr{B}_{67}}(z) = \left(1+z^{136}\right) + 66\cdot\left(z^{24}+z^{112}\right) + 682\cdot\left(z^{28}+z^{108}\right) + 3696\cdot\left(z^{32}+z^{104}\right) +$$
$$12390\cdot\left(z^{36}+z^{100}\right) + 54747\cdot\left(z^{40}+z^{96}\right) + 163680\cdot\left(z^{44}+z^{92}\right) +$$
$$318516\cdot\left(z^{48}+z^{88}\right) + 753522\cdot\left(z^{52}+z^{84}\right) + 1474704\cdot\left(z^{56}+z^{80}\right) +$$
$$1763454\cdot\left(z^{60}+z^{76}\right) + 2339502\cdot\left(z^{64}+z^{72}\right) + 3007296\cdot z^{68}$$

Table 9.12 Modular congruence weight distributions of $\mathscr{B}_{59}$

i	$A_i(S_2) \bmod 2^2$	$A_i(S_3) \bmod 3$	$A_i(S_5) \bmod 5$	$A_i(S_{29}) \bmod 29$	$A_i(S_{59}) \bmod 59$	$A_i(\mathscr{H}) \bmod 102660$	n_i [a]	A_i
0	1	1	1	1	1	1	0	1
20	2	0	2	0	0	71862	0	71862
24	3	0	0	0	0	76995	372	38266515
28	0	0	0	0	0	0	59565	6114942900
32	1	0	0	4	0	32745	4632400	475562216745
36	2	1	0	0	0	17110	183370922	18824858869630
40	0	0	1	0	0	61596	3871511775	397449398883096
44	0	0	0	0	0	0	45105349212	4630515150103920
48	0	0	0	0	0	0	297404962554	30531593455793640
52	0	0	0	0	0	0	1130177151411	116023986363853260
56	3	0	0	0	0	76995	2505920073120	257257754706576195
60	0	0	3	6	2	85788	3265149944551	335200293307691448
64	3	0	0	0	0	76995	2505920073120	257257754706576195
68	0	0	0	0	0	0	1130177151411	116023986363853260
72	0	0	0	0	0	0	297404962554	30531593455793640
76	0	0	0	0	0	0	45105349212	4630515150103920
80	0	0	1	0	0	61596	3871511775	397449398883096
84	2	1	0	0	0	17110	183370922	18824858869630
88	1	0	0	4	0	32745	4632400	475562216745
92	0	0	0	0	0	0	59565	6114942900
96	3	0	0	0	0	76995	372	38266515
100	2	0	2	0	0	71862	0	71862
120	1	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{102660}$

$$A^{(S_{11})}_{\mathscr{B}_{67}}(z) = \left(1 + z^{136}\right) + 6 \cdot \left(z^{24} + z^{112}\right) + 16 \cdot \left(z^{36} + z^{100}\right) + 6 \cdot \left(z^{44} + z^{92}\right) + 9 \cdot \left(z^{48} + z^{88}\right) + 48 \cdot \left(z^{56} + z^{80}\right) + 84 \cdot z^{68}$$

$$A^{(S_{17})}_{\mathscr{B}_{67}}(z) = \left(1 + z^{136}\right) + 14 \cdot z^{68}$$

$$A^{(S_{67})}_{\mathscr{B}_{67}}(z) = \left(1 + z^{136}\right) + 2 \cdot z^{68}$$

The weight distributions of $\mathscr{B}_{67}$ and their modular congruence are shown in Table 9.13.

Prime 83

We have $P = \left[\begin{smallmatrix} 1 & 9 \\ 9 & 82 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 82 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(83)$, and the permutations of order 3, 7, 41 and 83 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 10 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 4 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 82 & 81 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(83) = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83 \cdot = 285852$$

and the weight enumerator polynomials of the invariant subcodes are

$$\begin{aligned} A^{(G_2^0)}_{\mathscr{B}_{83}}(z) = {} & \left(1 + z^{168}\right) + 196 \cdot \left(z^{24} + z^{144}\right) + 1050 \cdot \left(z^{28} + z^{140}\right) + \\ & 29232 \cdot \left(z^{32} + z^{136}\right) + 443156 \cdot \left(z^{36} + z^{132}\right) + \\ & 4866477 \cdot \left(z^{40} + z^{128}\right) + 42512190 \cdot \left(z^{44} + z^{124}\right) + \\ & 292033644 \cdot \left(z^{48} + z^{120}\right) + 1590338568 \cdot \left(z^{52} + z^{116}\right) + \\ & 6952198884 \cdot \left(z^{56} + z^{112}\right) + 24612232106 \cdot \left(z^{60} + z^{108}\right) + \\ & 71013075210 \cdot \left(z^{64} + z^{104}\right) + 167850453036 \cdot \left(z^{68} + z^{100}\right) + \\ & 326369180312 \cdot \left(z^{72} + z^{96}\right) + 523672883454 \cdot \left(z^{76} + z^{92}\right) + \\ & 694880243820 \cdot \left(z^{80} + z^{88}\right) + 763485528432 \cdot z^{84} \end{aligned}$$

$$\begin{aligned} A^{(G_4)}_{\mathscr{B}_{83}}(z) = {} & \left(1 + z^{168}\right) + 4 \cdot \left(z^{24} + z^{144}\right) + 6 \cdot \left(z^{28} + z^{140}\right) + \\ & 96 \cdot \left(z^{32} + z^{136}\right) + 532 \cdot \left(z^{36} + z^{132}\right) + 1437 \cdot \left(z^{40} + z^{128}\right) + \\ & 3810 \cdot \left(z^{44} + z^{124}\right) + 10572 \cdot \left(z^{48} + z^{120}\right) + 24456 \cdot \left(z^{52} + z^{116}\right) + \\ & 50244 \cdot \left(z^{56} + z^{112}\right) + 95030 \cdot \left(z^{60} + z^{108}\right) + 158874 \cdot \left(z^{64} + z^{104}\right) + \\ & 241452 \cdot \left(z^{68} + z^{100}\right) + 337640 \cdot \left(z^{72} + z^{96}\right) + 425442 \cdot \left(z^{76} + z^{92}\right) + \\ & 489708 \cdot \left(z^{80} + z^{88}\right) + 515696 \cdot z^{84} \end{aligned}$$

Table 9.13 Modular congruence weight distributions of $\mathscr{B}_{67}$

i	$A_i(S_2) \bmod 2^2$	$A_i(S_3) \bmod 3$	$A_i(S_{11}) \bmod 11$	$A_i(S_{17}) \bmod 17$	$A_i(S_{67}) \bmod 67$	$A_i(\mathscr{H}) \bmod 150348$	n_i[a]	A_i
0	1	1	1	1	1	1	0	1
24	2	0	6	0	0	88842	26	3997890
28	0	1	0	0	0	50116	8173	1228844320
32	3	0	0	0	0	37587	1217081	182985731775
36	0	0	5	0	0	136680	95005682	14283914414016
40	1	0	0	0	0	112761	4076381478	612875802567105
44	0	0	6	0	0	13668	99752935189	14997654299809440
48	2	0	9	0	0	20502	1432445445981	215365307912371890
52	0	0	0	0	0	0	12338369112000	1855049119250976000
56	0	0	4	0	0	109344	64817708364545	9745212817192721004
60	0	0	0	0	0	0	210227711554224	31607315976754469952
64	3	0	0	0	0	37587	424499666112161	63822675800631219615
68	0	0	7	14	2	138156	536258660836183	80625417139398579840
72	3	0	0	0	0	37587	424499666112161	63822675800631219615
76	0	0	0	0	0	0	210227711554224	31607315976754469952
80	0	0	4	0	0	109344	64817708364545	9745212817192721004
84	0	0	0	0	0	0	12338369112000	1855049119250976000
88	2	0	9	0	0	20502	1432445445981	215365307912371890
92	0	0	6	0	0	13668	99752935189	14997654299809440
96	1	0	0	0	0	112761	4076381478	612875802567105
100	0	0	5	0	0	136680	95005682	14283914414016
104	3	0	0	0	0	37587	1217081	182985731775
108	0	1	0	0	0	50116	8173	1228844320
112	2	0	6	0	0	88842	26	3997890
136	1	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{150348}$

$$A^{(S_3)}_{\mathscr{B}_{83}}(z) = \left(1 + z^{168}\right) + 63 \cdot \left(z^{24} + z^{144}\right) + 8568 \cdot \left(z^{36} + z^{132}\right) + 617085 \cdot \left(z^{48} + z^{120}\right) + 11720352 \cdot \left(z^{60} + z^{108}\right) + 64866627 \cdot \left(z^{72} + z^{96}\right) + 114010064 \cdot z^{84}$$

$$A^{(S_7)}_{\mathscr{B}_{83}}(z) = \left(1 + z^{168}\right) + 759 \cdot \left(z^{56} + z^{112}\right) + 2576 \cdot z^{84}$$

$$A^{(S_{41})}_{\mathscr{B}_{83}}(z) = \left(1 + z^{168}\right) + 4 \cdot \left(z^{44} + z^{124}\right) + 6 \cdot z^{84}$$

$$A^{(S_{83})}_{\mathscr{B}_{83}}(z) = \left(1 + z^{168}\right) + 2 \cdot z^{84}.$$

The weight distributions of $\mathscr{B}_{83}$ and their modular congruence are shown in Table 9.14.

Primes −3 Modulo 8

Prime 13

We have $P = \left[\begin{smallmatrix} 3 & 4 \\ 4 & 10 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 12 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(13)$, and the permutations of order 3, 7 and 13 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 12 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 12 & 3 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 12 & 11 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(13) = 2^2 \cdot 3 \cdot 7 \cdot 13 \cdot = 1092$$

and the weight enumerator polynomials of the invariant subcodes are

$$A^{G_2^0}_{\mathscr{B}_{13}}(z) = \left(1 + z^{28}\right) + 26 \cdot \left(z^8 + z^{20}\right) + 32 \cdot \left(z^{10} + z^{18}\right) + 37 \cdot \left(z^{12} + z^{16}\right) + 64 \cdot z^{14}$$

$$A^{G_4}_{\mathscr{B}_{13}}(z) = \left(1 + z^{28}\right) + 10 \cdot \left(z^8 + z^{20}\right) + 8 \cdot \left(z^{10} + z^{18}\right) + 5 \cdot \left(z^{12} + z^{16}\right) + 16 \cdot z^{14}$$

$$A^{S_3}_{\mathscr{B}_{13}}(z) = \left(1 + z^{28}\right) + 6 \cdot \left(z^8 + z^{20}\right) + 10 \cdot \left(z^{10} + z^{18}\right) + 9 \cdot \left(z^{12} + z^{16}\right) + 12 \cdot z^{14}$$

$$A^{S_7}_{\mathscr{B}_{13}}(z) = \left(1 + z^{28}\right) + 2 \cdot z^{14}$$

$$A^{S_{13}}_{\mathscr{B}_{13}}(z) = \left(1 + z^{28}\right) + 2 \cdot z^{14}.$$

The weight distributions of $\mathscr{B}_{13}$ and their modular congruence are shown in Table 9.15.

Prime 29

We have $P = \left[\begin{smallmatrix} 2 & 13 \\ 13 & 27 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 28 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(29)$, and the permutations of order 3, 5, 7 and 29 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 28 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 28 & 5 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 28 & 3 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 28 & 27 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(29) = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot = 12180$$

Table 9.14 Modular congruence weight distributions of $\mathscr{D}_{83}$

i	$A_i(S_2)$	$A_i(S_3)$	$A_i(S_7)$	$A_i(S_{41})$	$A_i(S_{83})$	$A_i(\mathscr{H})$	n_i[a]	A_i
i	mod 2^2	mod 3	mod 7	mod 41	mod 83	mod 285852		
0	1	1	1	1	0	6889	0	1
24	0	0	0	0	0	0	2	571704
28	2	0	0	0	0	142926	59	17008194
32	0	0	0	0	0	0	19267	5507510484
36	0	0	0	0	0	0	4382043	1252615755636
40	1	0	0	0	0	214389	580925895	166058829151929
44	2	0	0	4	0	156870	45643181220	13047194638256310
48	0	0	0	0	0	0	2200608997142	629048483051034984
52	0	0	0	0	0	0	66772769854878	19087129808556586056
56	0	0	3	0	0	81672	1301721510043764	372099697089030108600
60	2	0	0	0	0	142926	16579528883596695	4739291490433882602066
64	2	0	0	0	0	142926	139840453892634544	39973673426117369814414
68	0	0	0	0	0	0	789557804450518101	225696677517789500207052
72	0	0	0	0	0	0	3009393355026378047	860241109321000217491044
76	2	0	0	0	0	142926	7792111592501736790	222739068293980646503 8006
80	0	0	0	0	0	0	13766213240696824038	393509958727966854491 0376
84	0	2	0	6	0	211484	16637096860279621422	475574741170465034320 5104
88	0	0	0	0	0	0	13766213240696824038	393509958727966854491 0376
92	2	0	0	0	0	142926	7792111592501736790	222739068293980646503 8006

(continued)

Table 9.14 (continued)

i	$A_i(S_2)$	$A_i(S_3)$	$A_i(S_7)$	$A_i(S_{41})$	$A_i(S_{83})$	$A_i(\mathscr{H})$	n_i[a]	A_i
i	mod 2^2	mod 3	mod 7	mod 41	mod 83	mod 285852		
96	0	0	0	0	0	0	3009393355026378047	860241109321000217491044
100	0	0	0	0	0	0	789557804450518101	22569667751778950020 7052
104	2	0	0	0	0	142926	139840453892634544	39973673426117369814414
108	2	0	0	0	0	142926	16579528883596695	4739291490433882602066
112	0	0	3	0	0	81672	1301721510043764	372099697089030108600
116	0	0	0	0	0	0	66772769854878	19087129808556586056
120	0	0	0	0	0	0	2200608997142	629048483051034984
124	2	0	0	4	0	156870	45643181220	13047194638256310
128	1	0	0	0	0	214389	580925895	166058829151929
132	0	0	0	0	0	0	4382043	1252615755636
136	0	0	0	0	0	0	19267	5507510484
140	2	0	0	0	0	142926	59	17008194
144	0	0	0	0	0	0	2	571704
168	1	1	1	1	0	6889	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{285852}$

Table 9.15 Modular congruence weight distributions of $\mathscr{B}_{13}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3	$A_i(S_7)$ mod 7	$A_i(S_{13})$ mod 13	$A_i(\mathscr{H})$ mod 1092	n_i[a]	A_i
0	1	1	1	1	1	0	1
8	2	0	0	0	546	0	546
10	0	1	0	0	364	1	1456
12	1	0	0	0	273	3	3549
14	0	0	2	2	912	4	5280
16	1	0	0	0	273	3	3549
18	0	1	0	0	364	1	1456
20	2	0	0	0	546	0	546
28	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{1092}$

and the weight enumerator polynomials of the invariant subcodes are

$$A^{(G_2^0)}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 28\cdot\left(z^{12}+z^{48}\right) + 112\cdot\left(z^{14}+z^{46}\right) + 394\cdot\left(z^{16}+z^{44}\right) + 1024\cdot\left(z^{18}+z^{42}\right) + 1708\cdot\left(z^{20}+z^{40}\right) + 3136\cdot\left(z^{22}+z^{38}\right) + 5516\cdot\left(z^{24}+z^{36}\right) + 7168\cdot\left(z^{26}+z^{34}\right) + 8737\cdot\left(z^{28}+z^{32}\right) + 9888\cdot z^{30}$$

$$A^{(G_4)}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 12\cdot\left(z^{14}+z^{46}\right) + 30\cdot\left(z^{16}+z^{44}\right) + 32\cdot\left(z^{18}+z^{42}\right) + 60\cdot\left(z^{20}+z^{40}\right) + 48\cdot\left(z^{22}+z^{38}\right) + 60\cdot\left(z^{24}+z^{36}\right) + 96\cdot\left(z^{26}+z^{34}\right) + 105\cdot\left(z^{28}+z^{32}\right) + 136\cdot z^{30}$$

$$A^{(S_3)}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 10\cdot\left(z^{12}+z^{48}\right) + 70\cdot\left(z^{18}+z^{42}\right) + 245\cdot\left(z^{24}+z^{36}\right) + 372\cdot z^{30}$$

$$A^{(S_5)}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 15\cdot\left(z^{20}+z^{40}\right) + 32\cdot z^{30}$$

$$A^{(S_7)}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 6\cdot\left(z^{16}+z^{44}\right) + 2\cdot\left(z^{18}+z^{42}\right) + 8\cdot\left(z^{22}+z^{38}\right) + 8\cdot\left(z^{24}+z^{36}\right) + 1\cdot\left(z^{28}+z^{32}\right) + 12\cdot z^{30}$$

$$A^{(S_{29})}_{\mathscr{B}_{29}}(z) = \left(1+z^{60}\right) + 2\cdot z^{30}.$$

The weight distributions of $\mathscr{B}_{29}$ and their modular congruence are shown in Table 9.16.

Prime 53

We have $P = \left[\begin{smallmatrix} 3 & 19 \\ 19 & 50 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 52 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(53)$, and the permutations of order 3, 13 and 53 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 52 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 52 & 8 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 52 & 51 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(53) = 2^2 \cdot 3^3 \cdot 13 \cdot 53 \cdot = 74412$$

Table 9.16 Modular congruence weight distributions of $\mathscr{B}_{29}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3	$A_i(S_5)$ mod 5	$A_i(S_7)$ mod 7	$A_i(S_{29})$ mod 29	$A_i(\mathscr{H})$ mod 12180	n_i[a]	A_i
0	1	1	1	1	1	1	0	1
12	0	1	0	0	0	4060	0	4060
14	0	0	0	0	0	0	2	24360
16	2	0	0	6	0	2610	24	294930
18	0	1	0	2	0	11020	141	1728400
20	0	0	0	0	0	0	637	7758660
22	0	0	0	1	0	3480	2162	26336640
24	0	2	0	1	0	11600	5533	67403540
26	0	0	0	0	0	0	10668	129936240
28	1	0	0	1	0	6525	15843	192974265
30	0	0	2	5	2	8412	18129	220819632
32	1	0	0	1	0	6525	15843	192974265
34	0	0	0	0	0	0	10668	129936240
36	0	2	0	1	0	11600	5533	67403540
38	0	0	0	1	0	3480	2162	26336640
40	0	0	0	0	0	0	637	7758660
42	0	1	0	2	0	11020	141	1728400
44	2	0	0	6	0	2610	24	294930
46	0	0	0	0	0	0	2	24360
48	0	1	0	0	0	4060	0	4060
60	1	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{12180}$

and the weight enumerator polynomials of the invariant subcodes are

$$
\begin{aligned}
A^{(G_2^0)}_{\mathscr{B}_{53}}(z) = {} & \left(1 + z^{108}\right) + 234 \cdot \left(z^{20} + z^{88}\right) + 1768 \cdot \left(z^{22} + z^{86}\right) + 5655 \cdot \left(z^{24} + z^{84}\right) + \\
& 16328 \cdot \left(z^{26} + z^{82}\right) + 47335 \cdot \left(z^{28} + z^{80}\right) + 127896 \cdot \left(z^{30} + z^{78}\right) + \\
& 316043 \cdot \left(z^{32} + z^{76}\right) + 705848 \cdot \left(z^{34} + z^{74}\right) + 1442883 \cdot \left(z^{36} + z^{72}\right) + \\
& 2728336 \cdot \left(z^{38} + z^{70}\right) + 4786873 \cdot \left(z^{40} + z^{68}\right) + 7768488 \cdot \left(z^{42} + z^{66}\right) + \\
& 11636144 \cdot \left(z^{44} + z^{64}\right) + 16175848 \cdot \left(z^{46} + z^{62}\right) + 20897565 \cdot \left(z^{48} + z^{60}\right) + \\
& 25055576 \cdot \left(z^{50} + z^{58}\right) + 27976131 \cdot \left(z^{52} + z^{56}\right) + 29057552 \cdot z^{54}
\end{aligned}
$$

$$
\begin{aligned}
A^{(G_4)}_{\mathscr{B}_{53}}(z) = {} & \left(1 + z^{108}\right) + 12 \cdot \left(z^{20} + z^{88}\right) + 12 \cdot \left(z^{22} + z^{86}\right) + 77 \cdot \left(z^{24} + z^{84}\right) + \\
& 108 \cdot \left(z^{26} + z^{82}\right) + 243 \cdot \left(z^{28} + z^{80}\right) + 296 \cdot \left(z^{30} + z^{78}\right) + 543 \cdot \left(z^{32} + z^{76}\right) + \\
& 612 \cdot \left(z^{34} + z^{74}\right) + 1127 \cdot \left(z^{36} + z^{72}\right) + 1440 \cdot \left(z^{38} + z^{70}\right) + 2037 \cdot \left(z^{40} + z^{68}\right) + \\
& 2636 \cdot \left(z^{42} + z^{66}\right) + 3180 \cdot \left(z^{44} + z^{64}\right) + 3672 \cdot \left(z^{46} + z^{62}\right) + 4289 \cdot \left(z^{48} + z^{60}\right) + \\
& 4836 \cdot \left(z^{50} + z^{58}\right) + 4875 \cdot \left(z^{52} + z^{56}\right) + 5544 \cdot z^{54}
\end{aligned}
$$

Table 9.17 Modular congruence weight distributions of $\mathscr{B}_{53}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3^3	$A_i(S_{13})$ mod 13	$A_i(S_{53})$ mod 53	$A_i(\mathscr{H})$ mod 74412	n_i[a]	A_i
0	1	1	1	1	1	0	1
20	2	0	0	0	37206	3	260442
22	0	0	0	0	0	78	5804136
24	3	18	0	0	43407	1000	74455407
26	0	0	0	0	0	10034	746650008
28	3	0	6	0	64395	91060	6776021115
30	0	18	2	0	64872	658342	48988609776
32	3	0	0	0	18603	3981207	296249593887
34	0	0	0	0	0	20237958	1505946930696
36	3	6	0	0	26871	86771673	6456853758147
38	0	0	0	0	0	315441840	23472658198080
40	1	0	8	0	67257	976699540	72678166237737
42	0	0	8	0	11448	2584166840	192293022909528
44	0	0	0	0	0	5859307669	436002802265628
46	0	0	0	0	0	11412955404	849260837522448
48	1	9	0	0	31005	19133084721	1423731100290057
50	0	0	0	0	0	27645086470	2057126174405640
52	3	0	1	0	1431	34462554487	2564427604488075
54	0	5	12	2	55652	37087868793	2759782492680368
56	3	0	1	0	1431	34462554487	2564427604488075
58	0	0	0	0	0	27645086470	2057126174405640
60	1	9	0	0	31005	19133084721	1423731100290057
62	0	0	0	0	0	11412955404	849260837522448
64	0	0	0	0	0	5859307669	436002802265628
66	0	0	8	0	11448	2584166840	192293022909528
68	1	0	8	0	67257	976699540	72678166237737
70	0	0	0	0	0	315441840	23472658198080
72	3	6	0	0	26871	86771673	6456853758147
74	0	0	0	0	0	20237958	1505946930696
76	3	0	0	0	18603	3981207	296249593887
78	0	18	2	0	64872	658342	48988609776
80	3	0	6	0	64395	91060	6776021115
82	0	0	0	0	0	10034	746650008
84	3	18	0	0	43407	1000	74455407
86	0	0	0	0	0	78	5804136
88	2	0	0	0	37206	3	260442
108	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{74412}$

Table 9.18 Modular congruence weight distributions of $\mathscr{B}_{61}$

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3	$A_i(S_5)$ mod 5	$A_i(S_{31})$ mod 31	$A_i(S_{61})$ mod 61	$A_i(\mathscr{H})$ mod 113460	n_i[a]	A_i
0	1	1	1	1	1	1	0	1
20	0	0	3	0	0	90768	0	90768
22	0	1	0	0	0	75640	4	529480
24	2	2	0	0	0	94550	95	10873250
26	0	2	4	0	0	83204	1508	171180884
28	2	2	3	0	0	71858	19029	2159102198
30	0	0	1	0	0	68076	199795	22668808776
32	0	1	0	0	0	75640	1759003	199576556020
34	0	0	3	0	0	90768	13123969	1489045613508
36	2	0	3	0	0	34038	83433715	9466389337938
38	0	1	1	0	0	30256	454337550	51549138453256
40	0	2	0	0	0	37820	2128953815	241551099887720
42	0	0	3	0	0	90768	8619600220	977979841051968
44	0	0	2	0	0	22692	30259781792	3433274842143012
46	0	2	1	0	0	105896	92387524246	10482288501057056
48	0	2	0	0	0	37820	245957173186	27906300869721380
50	0	2	0	0	0	37820	572226179533	64924782329852000
52	0	2	1	0	0	105896	1165598694540	132248827882614296
54	0	2	3	0	0	15128	2081950370302	236218089014480048
56	0	2	2	0	0	60512	3264875882211	370432817595720572
58	0	2	2	0	0	60512	4499326496930	510493584341738312
60	1	2	1	0	0	20801	5452574159887	618649064180799821
62	0	2	1	2	2	102116	5813004046431	659543439108163376
64	1	2	1	0	0	20801	5452574159887	618649064180799821
66	0	2	2	0	0	60512	4499326496930	510493584341738312
68	0	2	2	0	0	60512	3264875882211	370432817595720572
70	0	2	3	0	0	15128	2081950370302	236218089014480048
72	0	2	1	0	0	105896	1165598694540	132248827882614296
74	0	2	0	0	0	37820	572226179533	64924782329852000
76	0	2	0	0	0	37820	245957173186	27906300869721380
78	0	2	1	0	0	105896	92387524246	10482288501057056
80	0	0	2	0	0	22692	30259781792	3433274842143012
82	0	0	3	0	0	90768	8619600220	977979841051968
84	0	2	0	0	0	37820	2128953815	241551099887720
86	0	1	1	0	0	30256	454337550	51549138453256

(continued)

Table 9.18 (continued)

i	$A_i(S_2)$ mod 2^2	$A_i(S_3)$ mod 3	$A_i(S_5)$ mod 5	$A_i(S_{31})$ mod 31	$A_i(S_{61})$ mod 61	$A_i(\mathscr{H})$ mod 113460	n_i[a]	A_i
88	2	0	3	0	0	34038	83433715	9466389337938
90	0	0	3	0	0	90768	13123969	1489045613508
92	0	1	0	0	0	75640	1759003	199576556020
94	0	0	1	0	0	68076	199795	22668808776
96	2	2	3	0	0	71858	19029	2159102198
98	0	2	4	0	0	83204	1508	171180884
100	2	2	0	0	0	94550	95	10873250
102	0	1	0	0	0	75640	4	529480
104	0	0	3	0	0	90768	0	90768
124	1	1	1	1	1	1	0	1

[a] $n_i = \frac{A_i - A_i(\mathscr{H})}{113460}$

$$A^{(S_3)}_{\mathscr{B}_{53}}(z) = \left(1 + z^{108}\right) + 234 \cdot \left(z^{24} + z^{84}\right) + 1962 \cdot \left(z^{30} + z^{78}\right) + 9672 \cdot \left(z^{36} + z^{72}\right) + 28728 \cdot \left(z^{42} + z^{66}\right) + 55629 \cdot \left(z^{48} + z^{60}\right) + 69692 \cdot z^{54}$$

$$A^{(S_{13})}_{\mathscr{B}_{53}}(z) = \left(1 + z^{108}\right) + 6 \cdot \left(z^{28} + z^{80}\right) + 2 \cdot \left(z^{30} + z^{78}\right) + 8 \cdot \left(z^{40} + z^{68}\right) + 8 \cdot \left(z^{42} + z^{66}\right) + 1 \cdot \left(z^{52} + z^{56}\right) + 12 \cdot z^{54}$$

$$A^{(S_{53})}_{\mathscr{B}_{53}}(z) = \left(1 + z^{108}\right) + 2 \cdot z^{54}.$$

The weight distributions of $\mathscr{B}_{53}$ and their modular congruence are shown in Table 9.17.

Prime 61

We have $P = \left[\begin{smallmatrix} 2 & 19 \\ 19 & 59 \end{smallmatrix}\right]$ and $T = \left[\begin{smallmatrix} 0 & 60 \\ 1 & 0 \end{smallmatrix}\right]$, $P, T \in \mathrm{PSL}_2(61)$, and the permutations of order 3, 5, 31 and 61 are generated by $\left[\begin{smallmatrix} 0 & 1 \\ 60 & 1 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 60 & 17 \end{smallmatrix}\right]$, $\left[\begin{smallmatrix} 0 & 1 \\ 60 & 5 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} 0 & 1 \\ 60 & 59 \end{smallmatrix}\right]$, respectively. In addition,

$$\mathrm{PSL}_2(61) = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61 \cdot = 113460$$

and the weight enumerator polynomials of the invariant subcodes are

$$A^{(G_2^0)}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 208\cdot\left(z^{20}+z^{104}\right) + 400\cdot\left(z^{22}+z^{102}\right) + 1930\cdot\left(z^{24}+z^{100}\right) + 8180\cdot\left(z^{26}+z^{98}\right) + 26430\cdot\left(z^{28}+z^{96}\right) + 84936\cdot\left(z^{30}+z^{94}\right) + 253572\cdot\left(z^{32}+z^{92}\right) + 696468\cdot\left(z^{34}+z^{90}\right) + 1725330\cdot\left(z^{36}+z^{88}\right) + 3972240\cdot\left(z^{38}+z^{86}\right) + 8585008\cdot\left(z^{40}+z^{84}\right) + 17159632\cdot\left(z^{42}+z^{82}\right) + 31929532\cdot\left(z^{44}+z^{80}\right) + 55569120\cdot\left(z^{46}+z^{78}\right) + 90336940\cdot\left(z^{48}+z^{76}\right) + 137329552\cdot\left(z^{50}+z^{74}\right) + 195328240\cdot\left(z^{52}+z^{72}\right) + 260435936\cdot\left(z^{54}+z^{70}\right) + 325698420\cdot\left(z^{56}+z^{68}\right) + 381677080\cdot\left(z^{58}+z^{66}\right) + 419856213\cdot\left(z^{60}+z^{64}\right) + 433616560\cdot z^{62}$$

$$A^{(G_4)}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 12\cdot\left(z^{20}+z^{104}\right) + 12\cdot\left(z^{22}+z^{102}\right) + 36\cdot\left(z^{24}+z^{100}\right) + 40\cdot\left(z^{26}+z^{98}\right) + 140\cdot\left(z^{28}+z^{96}\right) + 176\cdot\left(z^{30}+z^{94}\right) + 498\cdot\left(z^{32}+z^{92}\right) + 576\cdot\left(z^{34}+z^{90}\right) + 1340\cdot\left(z^{36}+z^{88}\right) + 1580\cdot\left(z^{38}+z^{86}\right) + 2660\cdot\left(z^{40}+z^{84}\right) + 3432\cdot\left(z^{42}+z^{82}\right) + 4932\cdot\left(z^{44}+z^{80}\right) + 6368\cdot\left(z^{46}+z^{78}\right) + 8820\cdot\left(z^{48}+z^{76}\right) + 10424\cdot\left(z^{50}+z^{74}\right) + 12752\cdot\left(z^{52}+z^{72}\right) + 14536\cdot\left(z^{54}+z^{70}\right) + 15840\cdot\left(z^{56}+z^{68}\right) + 18296\cdot\left(z^{58}+z^{66}\right) + 18505\cdot\left(z^{60}+z^{64}\right) + 20192\cdot z^{62}$$

$$A^{(S_3)}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 30\cdot\left(z^{20}+z^{104}\right) + 10\cdot\left(z^{22}+z^{102}\right) + 50\cdot\left(z^{24}+z^{100}\right) + 200\cdot\left(z^{26}+z^{98}\right) + 620\cdot\left(z^{28}+z^{96}\right) + 960\cdot\left(z^{30}+z^{94}\right) + 2416\cdot\left(z^{32}+z^{92}\right) + 4992\cdot\left(z^{34}+z^{90}\right) + 6945\cdot\left(z^{36}+z^{88}\right) + 15340\cdot\left(z^{38}+z^{86}\right) + 25085\cdot\left(z^{40}+z^{84}\right) + 34920\cdot\left(z^{42}+z^{82}\right) + 68700\cdot\left(z^{44}+z^{80}\right) + 87548\cdot\left(z^{46}+z^{78}\right) + 104513\cdot\left(z^{48}+z^{76}\right) + 177800\cdot\left(z^{50}+z^{74}\right) + 201440\cdot\left(z^{52}+z^{72}\right) + 225290\cdot\left(z^{54}+z^{70}\right) + 322070\cdot\left(z^{56}+z^{68}\right) + 301640\cdot\left(z^{58}+z^{66}\right) + 316706\cdot\left(z^{60}+z^{64}\right) + 399752\cdot z^{62}$$

$$A^{(S_5)}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 3\cdot\left(z^{20}+z^{104}\right) + 24\cdot\left(z^{26}+z^{98}\right) + 48\cdot\left(z^{28}+z^{96}\right) + 6\cdot\left(z^{30}+z^{94}\right) + 150\cdot\left(z^{32}+z^{92}\right) + 8\cdot\left(z^{34}+z^{90}\right) + 168\cdot\left(z^{36}+z^{88}\right) + 96\cdot\left(z^{38}+z^{86}\right) + 75\cdot\left(z^{40}+z^{84}\right) + 468\cdot\left(z^{42}+z^{82}\right) + 132\cdot\left(z^{44}+z^{80}\right) + 656\cdot\left(z^{46}+z^{78}\right) + 680\cdot\left(z^{48}+z^{76}\right) + 300\cdot\left(z^{50}+z^{74}\right) + 1386\cdot\left(z^{52}+z^{72}\right) + 198\cdot\left(z^{54}+z^{70}\right) + 1152\cdot\left(z^{56}+z^{68}\right) + 1272\cdot\left(z^{58}+z^{66}\right) + 301\cdot\left(z^{60}+z^{64}\right) + 2136\cdot z^{62}$$

$$A^{(S_{31})}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 2\cdot z^{62}$$

$$A^{(S_{61})}_{\mathscr{B}_{61}} = \left(1+z^{124}\right) + 2\cdot z^{62}$$

The weight distributions of $\mathscr{B}_{61}$ and their modular congruence are shown in Table 9.18.

Weight Distributions of Quadratic Residues Codes for Primes 151 and 167

See Tables 9.19 and 9.20

Table 9.19 Weight distributions of QR and extended QR codes of prime 151

i	A_i of [152, 76, 20] code	$\mathscr{A}_i$ of [151, 76, 19] code
0	1	1
19	0	3775
20	28690	24915
23	0	113250
24	717250	604000
27	0	30256625
28	164250250	133993625
31	0	8292705580
32	39390351505	31097645925
35	0	1302257122605
36	5498418962110	4196161839505
39	0	113402818847850
40	430930711621830	317527892773980
43	0	5706949034630250
44	19714914846904500	14007965812274250
47	0	171469716029462700
48	542987434093298550	371517718063835850
51	0	3155019195317144883
52	9222363801696269658	6067344606379124775
55	0	36274321608490644595
56	98458872937331749615	62184551328841105020
59	0	264765917968736096775
60	670740325520798111830	405974407552062015055
63	0	1241968201959417159800
64	2949674479653615754525	1707706277694198594725
67	0	3778485133479463579225
68	844602559248350682 4150	466754045900404324 4925
71	0	7503425412744902320620
72	15840564760239238232420	8337139347494335911800
75	0	9763682329503348632684
76	19527364659006697265368	9763682329503348632684

Table 9.20 Weight distributions of QR and extended QR codes of prime 167

i	A_i of [168, 84, 24] code	$\mathscr{A}_i$ of [167, 84, 23] code
0	1	1
23	0	110888
24	776216	665328
27	0	3021698
28	18130188	15108490
31	0	1057206192
32	5550332508	4493126316
35	0	268132007628
36	1251282702264	983150694636
39	0	39540857275985
40	166071600559137	126530743283152
43	0	3417107288264670
44	13047136918828740	9630029630564070
47	0	179728155397349776
48	629048543890724216	449320388493374440
51	0	5907921405841809432
52	19087130695796615088	13179209289954805656
55	0	124033230083117023704
56	372099690249351071112	248066460166234047408
59	0	1692604114105553659010
60	4739291519495550245228	3046687405389996586218
63	0	15228066033367763990128
64	3997367333759038047 4086	2474560730422261648 3958
67	0	91353417175290660468884
68	2256966777271886905 70184	1343432605518980301013 00
71	0	3686747609665117465490 04
72	8602411089218607419476 76	4915663479553489953986 72
75	0	1007629118755817710057646
76	2227390683565491780127428	1219761564809674070069782
79	0	1873856945935044844028880
80	3935099586463594172460648	2061242640528549328431768
83	0	2377873706297857672084688
84	4755747412595715344169376	2377873706297857672084688

References

1. Dougherty, T.G., Harada, M.: Extremal binary self-dual codes. IEEE Trans. Inf. Theory **43**(6), 2036–2047 (1997)
2. Gaborit, P.: Quadratic double circulant codes over fields. J. Comb. Theory Ser. A **97**, 85–107 (2002)
3. Gaborit, P., Otmani, A.: Tables of self-dual codes (2007). http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html
4. Gaborit, P., Nedeloaia, C.S., Wassermann, A.: On the weight enumerators of duadic and quadratic residue codes. IEEE Trans. Inf. Theory **51**(1), 402–407 (2005)
5. Grassl, M.: On the minimum distance of some quadratic residue codes. In: Proceedings of the IEEE International Symposium on Inform. Theory, Sorento, Italy, p. 253 (2000)
6. Gulliver, T.A., Senkevitch, N.: On a class of self-dual codes derived from quadratic residue. IEEE Trans. Inf. Theory **45**(2), 701–702 (1999)
7. Huffman, W.C., Pless, V.S.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003) ISBN 0 521 78280 5
8. Jenson, R.: A double circulant presentation for quadratic residue codes. IEEE Trans. Inf. Theory **26**(2), 223–227 (1980)
9. Karlin, M.: New binary coding results by circulants. IEEE Trans. Inf. Theory **15**(1), 81–92 (1969)
10. Karlin, M., Bhargava, V.K., Tavares, S.E.: A note on the extended quadratic residue codes and their binary images. Inf. Control **38**, 148–153 (1978)
11. Leon, J.S.: A probabilistic algorithm for computing minimum weights of large error-correcting codes. IEEE Trans. Inf. Theory **34**(5), 1354–1359 (1988)
12. Leon, J.S., Masley, J.M., Pless, V.: Duadic codes. IEEE Trans. Inf. Theory **30**(5), 709–713 (1984)
13. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977)
14. Mykkeltveit, J., Lam, C., McEliece, R.J.: On the weight enumerators of quadratic residue codes. JPL Tech. Rep. 32-1526 **XII**, 161–166 (1972)
15. Rains, E.M., Sloane, N.J.A.: Self-dual codes. In: Pless, V.S., Huffman, W.C. (eds.) Handbook of Coding Theory. Elsevier, North Holland (1998)
16. Shannon, C.E.: Probability of error for optimal codes in a Gaussian channel. Bell. Syst. Tech. J. **38**(3), 611–656 (1959)
17. Tjhai, C.J.: A study of linear error correcting codes. Ph.D dissertation, University of Plymouth, UK (2007)
18. van Dijk, M., Egner, S., Greferath, M., Wassermann, A.: On two doubly even self-dual binary codes of length 160 and minimum weight 24. IEEE Trans. Inf. Theory **51**(1), 408–411 (2005)
19. van Lint, J.H.: Coding Theory. Lecture Notes in Mathematics vol. 201. Springer, Berlin (1970)
20. Zimmermann, K.H.: Integral hecke modules, integral generalized reed-muller codes, and linear codes. Technical Report, Technische Universität Hamburg-Harburg, Hamburg, Germany, pp. 3–96 (1996)