NON-EXISTENCE OF SOME NEARLY PERFECT SEQUENCES, NEAR BUTSON-HADAMARD MATRICES, AND NEAR CONFERENCE MATRICES

ARNE WINTERHOF, OĞUZ YAYLA, AND VOLKER ZIEGLER

Abstract. In this paper we study the non-existence problem of (nearly) perfect (almost) m-ary sequences via their connection to (near) Butson-Hadamard (BH) matrices and (near) conference matrices. Firstly, we apply a result on vanishing sums of roots of unity and a result of Brock on the unsolvability of certain equations over a cyclotomic number field to derive non-existence results for near BH matrices and near conference matrices. Secondly, we refine the idea of Brock in the case of cyclotomic number fields whose ring of integers is not a principal ideal domains and get many new non-existence results.

1. Introduction

For an integer $m \geq 2$ let ζ_m denote a primitive complex m-th root of unity. We call a v-periodic sequence $\underline{a} = (a_0, a_1, \dots, a_{v-1}, \dots)$ an *m-ary sequence* if $a_0, a_1, \dots, a_{v-1} \in \mathcal{E}_m = \{1, \zeta_m, \zeta_m^2, \dots, \zeta_m^{m-1}\}$ and an *almost m-ary sequence* if $a_0 = 0$ and $a_1, \dots, a_{v-1} \in \mathcal{E}_m$.

For $0 \leq t \leq v-1$, the *autocorrelation function* $C_{\underline{a}}(t)$ is defined by

$$C_{\underline{a}}(t) = \sum_{i=0}^{v-1} a_i \overline{a_{i+t}},$$

where $\overline{a}$ is the complex conjugate of a.

An m-ary or almost m-ary sequence $\underline{a}$ of period v is called a *perfect sequence* (PS) if $C_{\underline{a}}(t) = 0$ for all $1 \leq t \leq v-1$. Similarly, an almost m-ary sequence $\underline{a}$ of period v is called a *nearly perfect sequence* (NPS) of type $\gamma \in \{-1, +1\}$ if $C_{\underline{a}}(t) = \gamma$ for all $1 \leq t \leq v-1$. We extend this definition to any $\gamma \in \mathbb{Z}[\zeta_m] \cap \mathbb{R}$ with "small" absolute value with respect to n.

PS and NPS have several applications such as signal processing and radar, see for example [1, 4] and references therein.

PS and NPS can be identified with circulant near Butson-Hadamard matrices and conference matrices. A square matrix H of order v with entries in $\mathcal{E}_m$ is called a *near Butson-Hadamard matrix* $\mathrm{BH}_\gamma(v,m)$ of type γ if $H\overline{H}^T = (v-\gamma)I + \gamma J$ for a $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$. A $\mathrm{BH}_0(v,m)$ is called *Butson-Hadamard matrix* and a $\mathrm{BH}_0(v,2)$ is a *Hadamard matrix*. A square matrix C of order v with 0 on the diagonal and all off-diagonal entries in $\mathcal{E}_m$ is called a *near conference matrix* $\mathrm{C}_\gamma(v,m)$ of type γ if $C\overline{C}^T = (v-1-\gamma)I + \gamma J$ for a $\gamma \in \mathbb{R} \cap \mathbb{Z}[\zeta_m]$. A $\mathrm{C}_0(v,m)$ is called *conference matrix*. A square matrix $H = (h_{ij})$ of order v is called *circulant* if $h_{i+1 \bmod v, j+1 \bmod v} = h_{i,j}$ for all $0 \leq i,j < v$.

In this paper we prove several new non-existence results on $BH_\gamma(v,m)$ and $\mathrm{C}_\gamma(v,m)$ which can be interpreted as non-existence results for PS and NPS. For earlier non-existence results on PS and NPS see [3, 6, 7] and on Butson-Hadamard matrices [2, 9].

First, in Section 2 and 3 we derive some new non-existence results on $BH_\gamma(v,m)$ and $\mathrm{C}_\gamma(v,m)$ using well-known methods. However, in Section 4 we present a new idea which works for all m such that $\mathbb{Z}[\zeta_m]$ is not a principal ideal domain (e.g. $m = 23, 29, 31, 37, 39, 41, 43, 46, 47, 49, \dots$) and obtain some non-existence results which could not be obtained by the other methods before.

In the last section we interpret the results on $BH_\gamma(v,m)$ and $\mathrm{C}_\gamma(v,m)$ as results on PS and NPS and complete earlier tables for non-existence parameters.

2010 *Mathematics Subject Classification.* 94A55 05B20.

Key words and phrases. nearly perfect sequences, near Butson-Hadamard matrices, near conference matrices, cyclotomic number fields, ideal decomposition.

2. A result based on vanishing sums of roots of unity

In this section we present a non-existence result on $\mathrm{BH}_\gamma(v,m)$ and $\mathrm{C}_\gamma(v,m)$ based on the following result on vanishing sums of roots of unity due to Lam and Leung [5].

Proposition 2.1. *Let m be an integer with prime factorization $m = p_1^{a_1} p_2^{a_2} \dots p_\ell^{a_\ell}$. If there are m-th roots of unity $\xi_1, \xi_2, \dots, \xi_v$ with $\xi_1 + \xi_2 + \dots + \xi_v = 0$, then $v = p_1 t_1 + p_2 t_2 + \dots + p_\ell t_\ell$ with non-negative integers $t_1, t_2, \dots, t_\ell$.*

Remark. For the case that $m = p^a$ is the power of a prime p see also [9]. In this case, if there is a vanishing sum of v m-th roots of unity, v must be divisible by p and infinitely many v are excluded. However, if m is divisible by at least two primes $p_1 \neq p_2$, any sufficiently large v is of the form $v = t_1 p_1 + t_2 p_2$ with non-negative integers t_1 and t_2 and Proposition 2.1 excludes only a finite number of small v. In particular, if m is divisible by 6 only $v = 1$ is excluded.

An immediate consequence of Proposition 2.1 is the following corollary.

Corollary 2.2. *Let m be a positive integer with prime factorization $m = p_1^{a_1} p_2^{a_2} \dots p_\ell^{a_\ell}$ and $-\gamma$ be a sum of g m-th roots of unity. (Note that g is not unique.) Then a $\mathrm{BH}_\gamma(v,m)$ exists only if $v + g = p_1 t_1 + p_2 t_2 + \dots + p_\ell t_\ell$ for some non-negative integers $t_1, t_2, \dots, t_\ell$ and a $\mathrm{C}_\gamma(v,m)$ exists only if $v - 2 + g = p_1 t_1 + p_2 t_2 + \dots + p_\ell t_\ell$ for some non-negative integers $t_1, t_2, \dots, t_\ell$. If γ is an integer, then we can choose $g = -\gamma + m\dfrac{\gamma + |\gamma|}{2}$.*

Proof. Suppose that $H = (h_{i,j})$ is a $\mathrm{BH}_\gamma(v,m)$ (resp. $\mathrm{C}_\gamma(v,m)$), then

$$\sum_{i=0}^{v-1} h_{i,j}\overline{h_{k,i}} - \gamma = 0, \quad k \neq j.$$

So, by Proposition 2.1 we get the first part of the theorem. For the second part let γ be an integer. If $\gamma \le 0$, we can choose $g = -\gamma$. If $\gamma > 0$, then we use $-1 = \sum_{i=1}^{m-1} \zeta_m^i$, where ζ_m is any primitive m-th root of unity, and can choose $g = (m-1)\gamma$. □

Example. We performed an exhaustive search on all 4×4 5-ary circulant matrices for checking the existence of a circulant $\mathrm{BH}_\gamma(4,5)$. We obtain that a circulant $\mathrm{BH}_\gamma(4,5)$ exists only for $\gamma \in \{-1, -\zeta_5^3 - \zeta_5^2 + 1, \zeta_5^3 + \zeta_5^2 + 2, 4\}$. We note that for these circulant $\mathrm{BH}_\gamma(4,5)$ we can choose values of g in $\{1, 6, 16, 16\}$. Obviously, $v + g$ is always divisible by 5. In addition, we note that $|\zeta_5^3 + \zeta_5^2 + 2| \approx 0.38$, hence one can obtain a circulant $\mathrm{BH}_\gamma(4,5)$ for a nonzero γ such that $|\gamma| < 1$.

3. A result based on a self-conjugacy condition

In this section we present non-existence results on $\mathrm{BH}_\gamma(v,m)$ and $\mathrm{C}_\gamma(v,m)$ based on results of Brock [2].

Let p be a prime and m a positive integer with $\gcd(p,m) = 1$. We say that p is *self-conjugate* modulo m if the order f of p modulo m is even and $p^{f/2} \equiv -1 \bmod m$. Corollary 3.1 below is based on the fact that for a positive integer w there exists no solution α to the equation $\alpha\overline{\alpha} = w$ over $\mathbb{Q}[\zeta_m]$ if the square-free part of w is divisible by a prime which is self-conjugate modulo m, see [2, Theorem 3.1]. More precisely, [2, Theorem 2.5] implies:

- If there is a $\mathrm{BH}_\gamma(v,m)$, there is $\alpha \in \mathbb{Q}(\zeta_m)$ with

$$\alpha\overline{\alpha} = w_1,$$

where

$$w_1 = \begin{cases} (\gamma+1)v - \gamma, & v \text{ odd}, \\ ((\gamma+1)v - \gamma)(v - \gamma), & v \text{ even}. \end{cases} \tag{1}$$

- If there is a $C_\gamma(v,m)$, there is $\alpha \in \mathbb{Q}(\zeta_m)$ with
$$\alpha\overline{\alpha} = w_2,$$
where
$$w_2 = \begin{cases} (v-1)(\gamma+1), & v \text{ odd}, \\ (v-1)(\gamma+1)(v-1-\gamma), & v \text{ even}. \end{cases} \tag{2}$$

Now [2, Theorem 3.1] immediately implies the following result.

Corollary 3.1. *Let v, m be positive integers and $\gamma \in \mathbb{Z}$. Let v_1 (resp. v_2) be the square-free part of w_1 (resp. w_2) defined by (1) (resp. (2)). If there is a prime divisor p of v_1 (resp. v_2) such that p is self-conjugate modulo m, then there exists no $\mathrm{BH}_\gamma(v,m)$ (resp. $C_\gamma(v,m)$).*

Remark. (i) If $\gamma < -1$, there is neither a $\mathrm{BH}_\gamma(v,m)$ nor a $C_\gamma(v,m)$ since w_1 and w_2 are negative but $\alpha\overline{\alpha}$ is non-negative.
(ii) For $\mathrm{BH}_0(v,m)$ Corollary 3.1 is [2, Theorem 4.2 (i)].
(iii) Let p be a prime and $m = q^r$ or $m = 2q^r$ for a prime $q \equiv 3 \bmod 4$ with $\gcd(p,q) = 1$ (that is $\varphi(m)/2$ is odd, where φ denotes Euler's totient function). If p is a quadratic non-residue modulo q, then p is self-conjugate modulo m. Hence, Corollary 3.1 generalizes [9, Theorem 5] which deals with $\mathrm{BH}_0(v,q^r)$ and $\mathrm{BH}_0(v,2q^r)$ with a prime $q \equiv 3 \bmod 4$.

4. Results using prime ideal decomposition over cyclotomic fields

In this section we refine the idea of Brock [2]. We use the ideal decomposition of the principal ideal of a rational integer over the cyclotomic number field $\mathbb{Q}(\zeta_m)$ to find more values w for which the equation $\alpha\overline{\alpha} = w$ has no solution in $\mathbb{Z}[\zeta_m]$ which excludes the existence of several $\mathrm{BH}_\gamma(v,m)$ and $C_\gamma(v,m)$.

More precisely, let H be a $\mathrm{BH}_\gamma(v,m)$ for some integer γ. Then, $H\overline{H}^T = (v-\gamma)I + \gamma J$, $\det(H) \in \mathbb{Z}[\zeta_m]$ and $\det(H\overline{H}^T) = \det(H)\overline{\det(H)} = ((\gamma+1)v-\gamma)(v-\gamma)^{v-1}$. Therefore, we want to find criteria for the unsolvability of the equation
$$\alpha\overline{\alpha} = ((\gamma+1)v-\gamma)(v-\gamma)^{v-1} \tag{3}$$
over $\mathbb{Z}[\zeta_m]$. Analogously, there is no $C_\gamma(v,m)$ for some integer γ if
$$\alpha\overline{\alpha} = (\gamma+1)(v-1)(v-1-\gamma)^{v-1} \tag{4}$$
has no solution $\alpha \in \mathbb{Z}[\zeta_m]$.

Note that Brock [2] studied such equations over $\mathbb{Q}(\zeta_m)$ instead of $\mathbb{Z}[\zeta_m]$, where it was allowed to cancel squares. The following example shows that $\alpha\overline{\alpha} = w$ for some positive integer w may have a solution $\alpha \in \mathbb{Q}(\zeta_m)$ even if there is none in $\mathbb{Z}[\zeta_m]$.

Example. We have $\alpha\overline{\alpha} = 2$ with $\alpha = \frac{3+\sqrt{-23}}{4} \in \mathbb{Q}(\sqrt{-23}) \le \mathbb{Q}(\zeta_{23})$. However, there is no solution $\alpha \in \mathbb{Z}[\zeta_{23}]$ since $(2) = (2, \frac{1+\sqrt{-23}}{2})(2, \frac{1-\sqrt{-23}}{2})$ is product of two non-principal prime ideals in $\mathbb{Z}[\zeta_{23}]$.

We now present a simple criterion for the unsolvability of $\alpha\overline{\alpha} = w$ over $\mathbb{Z}[\zeta_m]$ if $\mathbb{Z}[\zeta_m]$ is not a principal ideal domain. We denote by h_m the class number of the cyclotomic number field $\mathbb{Q}(\zeta_m)$ (and assume $h_m \ge 2$ in the following).

Theorem 4.1. *Let $t \ge 1$ and $e \ge 0$ be rational integers and q be a rational prime such that $q \nmid t$,*
$$\mathrm{ord}_m(q) = \varphi(m)/2. \tag{5}$$
and $\gcd(2e+1-2k, h_m) = 1$ for all integers $0 \le k \le e-1$. Then the equation
$$\alpha\overline{\alpha} = tq^{2e+1} \tag{6}$$
has no solution over $\mathbb{Z}[\zeta_m]$, provided that every prime ideal $\mathfrak{t} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{t}|(t)$ is principal and every prime ideal $\mathfrak{q} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{q}|(q)$ is non-principal.

TABLE 1. The class number h_m of $\mathbb{Q}(\zeta_m)$ for $m \le 70$ [8].

m	h_m	m	h_m	m	h_m	m	h_m	m	h_m	m	h_m	m	h_m
1	1	11	1	21	1	31	9	41	121	51	5	61	76301
2	1	12	1	22	1	32	1	42	1	52	3	62	9
3	1	13	1	23	3	33	1	43	211	53	48891	63	7
4	1	14	1	24	1	34	1	44	1	54	1	64	17
5	1	15	1	25	1	35	1	45	1	55	10	65	64
6	1	16	1	26	1	36	1	46	3	56	2	66	1
7	1	17	1	27	1	37	37	47	695	57	9	67	853513
8	1	18	1	28	1	38	1	48	1	58	8	68	8
9	1	19	1	29	8	39	2	49	43	59	41421	69	69
10	1	20	1	30	1	40	1	50	1	60	1	70	1

Proof. Assume that there exists a solution α to (6). We consider the prime ideal decomposition over $\mathbb{Q}(\zeta_m)$ of the right hand side of (6). According to [8, Theorem 2.13] we have $(q) = \mathfrak{q}_1 \dots \mathfrak{q}_g$, where $g = \varphi(m)/\mathrm{ord}_m(q)$ and $g = 2$ by (5).

We may assume that

$$(\alpha) = \mathfrak{t}\mathfrak{q}_1^{2e+1-k}\mathfrak{q}_2^k = \mathfrak{t}\mathfrak{q}_1^{2e+1-2k}(\mathfrak{q}_1\mathfrak{q}_2)^k, \tag{7}$$

where $\mathfrak{t}|(t)$ is a principal ideal and k is some integer with $0 \le k \le e-1$. Since $(\mathfrak{q}_1\mathfrak{q}_2) = (q)$ is principal, the right hand side of (7) is principal only if $\mathfrak{q}_1^{2e+1-2k}$ is principal. Then, the order of $\mathfrak{q}_1$ is a divisor of $\gcd(2e+1-2k, h_m) = 1$, contradicting that $\mathfrak{q}_1$ is non-principal. □

Example.
- $\alpha\overline{\alpha} = 73$ has no solution $\alpha \in \mathbb{Z}[\zeta_{23}]$ since $(73) = (73, (1+\sqrt{-73})/2)(73, (1-\sqrt{-73})/2)$ over $\mathbb{Z}[\zeta_{23}]$ and $ord_{23}(73) = 11 = \varphi(23)/2$.
- $\alpha\overline{\alpha} = 3^3$ has no solution $\alpha \in \mathbb{Z}[\zeta_{47}]$ since $(3) = (3, (1+\sqrt{-47})/2)(3, (1-\sqrt{-47})/2)$ is a product of two non-principal prime ideals in $\mathbb{Z}[\zeta_{47}]$ and $h_{47} = 695$ is not divisible by 3.

Applying Theorem 4.1 to (3), we get a criterion for the non-existence of $\mathrm{BH}_\gamma(v,m)$:

Corollary 4.2. *Let v, m be positive integers and $\gamma \ge -1$ be an integer such that $((\gamma+1)v - \gamma)(v-\gamma)^{v-1} = tq^{2e+1}$ with integers $t \ge 1$ and $e \ge 0$ such that* $\gcd(2e+1-2k, h_m) = 1$ *for all integers $0 \le k \le e-1$, a prime q with* $\gcd(t,q) = 1$ *and* $\mathrm{ord}_m(q) = \varphi(m)/2$. *Let every prime ideal $\mathfrak{t} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{t}|(t)$ be principal and every prime ideal $\mathfrak{q} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{q}|(q)$ be non-principal. Then there exists no* $\mathrm{BH}_\gamma(v,m)$.

Remark.
(i) If $m = p^f$ is a prime power and $\mathrm{ord}_m(q)$ is even, then q is self conjugate modulo m and a $\mathrm{BH}(v,m)$ does not exist due to Brock [2] (cf. Corollary 3.1). Thus in the prime power case we consider only $\mathrm{BH}_\gamma(v,m)$ such that $\mathrm{ord}_m(q) = \varphi(m)/2$ is odd, i.e. $p \equiv 3 \bmod 4$.
(ii) We know by Corollary 2.2 that if a $\mathrm{BH}_\gamma(v,p^f)$ exists, then $p \mid v-\gamma$, and if a $\mathrm{BH}_\gamma(v,2p^f)$ exists then $v - \gamma = 2t_1 + pt_2$ for some non-negative integers t_1 and t_2.

Example. $\mathrm{BH}_2(25,23), \mathrm{BH}_2(117,23), \mathrm{BH}_2(163,23), \mathrm{BH}_1(32,31)$ do not exist by Corollary 4.2. The existence of $\mathrm{BH}_2(v,46)$ for $v \in \{25, 51, 55, 109, 111, 117, 163, 183, 193, 201, 213, 225, 247, 315, 363, 385, 433, 477\}$ such that $v \le 500$ are excluded by Corollary 4.2. Similarly, $\mathrm{BH}_2(v,72)$ for $v \in \{35, 141, 181, 183, 221, 231, 243, 245, 251, 395, 431, 475\}$ such that $v \le 500$ are excluded by Corollary 4.2. These matrices are the smallest examples whose existence cannot be excluded by Corollary 2.2 or Corollary 3.1. Finally, the existence of $\mathrm{BH}_2(115,94)$ can be excluded by Corollary 4.2, but not by Corollary 2.2 or Corollary 3.1.

Similarly to Corollary 4.2, applying Theorem 4.1 to (4), we get a criterion for the non-existence of $\mathrm{C}_\gamma(v,m)$:

Corollary 4.3. *Let v, m be positive integers and $\gamma \ge -1$ be an integer such that $(\gamma+1)(v-1)(v-1-\gamma)^{v-1} = tq^{2e+1}$ with integers $t \ge 1$ and $e \ge 0$ such that* $\gcd(2e+1-2k, h_m) = 1$ *for all* *integers $0 \le k \le e-1$, a prime q with $\gcd(t,q)=1$ and $\mathrm{ord}_m(q)=\varphi(m)/2$. Let every prime ideal $\mathfrak{t} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{t}|(t)$ be principal and every prime ideal $\mathfrak{q} \lhd \mathbb{Z}[\zeta_m]$ with $\mathfrak{q}|(q)$ be non-principal. Then there exists no $\mathrm{C}_\gamma(v,m)$.*

Remark. (i) In the cases $\gamma = 0$ and $h_m|v$ or $2|v$, or $\gamma = -1$, Corollary 4.3 does not yield a non-existence result for near conference matrices.

(ii) We know by Corollary 2.2 that if a $\mathrm{C}_\gamma(v,p^f)$ exists, then $p \mid v-2-\gamma$, and if $\mathrm{C}_\gamma(v,2p^f)$ exists, then $v-2-\gamma = 2t_1 + pt_2$ for some nonnegative integers t_1 and t_2.

Example. $\mathrm{C}_2(3362,23), \mathrm{C}_2(26,46), \mathrm{C}_2(124,72)$ do not exist by using Corollary 4.3. These matrices are the smallest examples whose existence cannot be excluded by Corollary 2.2 or Corollary 3.1.

5. Application to sequences

In this section we apply the results of the previous sections on matrices to sequences. We note that a NPS of type $\gamma = 0$ refers to a PS.

We start with the new results on the non-existence of m-ary NPS by using Corollary 3.1. We list in Table 2 all periods $v \le 100$ such that no m-ary NPS exists for $m \le 100$. We list only the new non-existence results. The pairs (v,m) listed in [6] such that an m-ary NPS of period v does not exist are not listed again in Table 2. In other words, we extend the tables in [6] for composite values of $m \le 100$.

We note that a 21-ary PS of period 105 does not exist by using Corollary 3.1. It differs from the other pairs in the first row of Table 2 as 21 is product of distinct primes. One of the smallest undecided cases is whether a 6-ary NPS of period $11, 12, 13$ for $\gamma = -1, 0, 1$, respectively, exists.

Similarly, we present non-existence results of almost m-ary NPS by using Corollary 3.1. We list in Table 3 all periods $v \le 100$ such that an almost m-ary NPS does not exist for $m \le 100$. We only list new non-existence results. The pairs (v,m) listed in [3] such that an almost m-ary NPS of period v does not exist are not listed again in Table 3. In particular, we extend the tables in [3] to composite $m \le 100$. We note that Corollary 3.1 does not yield any non-existence result for $\gamma = -1$ as the determinant vanishes. Finally, let us note that one of the smallest open cases is whether an almost 6-ary NPS of period $13, 14, 15$ for $\gamma = -1, 0, 1$ respectively, exists.

In addition, by using Corollary 4.2, we conclude that a 23-ary NPS of periods 25, 117 and 163 for $\gamma = 2$ and a 31-ary NPS of period 32 for $\gamma = 1$ do not exist. Similarly, by using Corollary 4.3, no almost 23-ary NPS of period 3362 for $\gamma = 2$ exists.

Acknowledgment

The first author is supported by the Austrian Science Fund (FWF): Project F5511-N26 which is part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". The second author is supported by TÜBİTAK under Grant No. 2219. The last author is supported by the Austrian Science Fund (FWF) under the project P24801-N26. We also want to thank Clemens Heuberger for several fruitful discussions on this topic during the special semester on Applications of Algebra and Number Theory held at the Johann Radon Institute for Computational and Applied Mathematics (RICAM) in Linz, October 14 - December 13, 2013.

Table 2. Periods $v \le 100$ such that an m-ary NPS does not exist.

	(v,m)
$\gamma = 0$	(45,9), (75,25), (99,9)
$\gamma = -1$	(44,9), (74,25), (98,9)
$\gamma = 1$	(11,10), (17,4), (26,25), (28,9), (28,27), (29,4), (29,14), (29,28), (35,34), (43,6), (43,14), (43,21), (43,42), (46,9), (53,4), (53,26), (59,58), (65,4), (67,22), (71,10), (71,14), (73,6), (73,9), (73,18), (76,25), (81,4), (81,8), (81,10), (83,82), (89,4), (93,46), (94,93), (100,9)

TABLE 3. Periods $v \leq 100$ such that an almost m-ary NPS does not exist.

	(v, m)
$\gamma = 0$	(11,9), (27,25), (35,33), (47,9), (59,57), (67,65), (71,69), (77,25), (79,77), (83,9), (83,27), (83,81),
$\gamma = 1$	(6,3), (7,2), (7,4), (8,5), (11,2), (12,3), (12,9), (13,2), (13,5), (13,10), (14,11), (15,2), (15,4), (16,13), (18,3), (18,5), (20,17), (21,2), (21,3), (21,6), (21,9), (21,18), (22,19), (23,2), (23,4), (24,3), (25,2), (27,2), (28,5), (28,25), (29,2), (29,13), (29,26), (30,3), (30,9), (30,27), (31,2), (31,4), (31,7), (31,14), (31,28), (32,29), (34,31), (35,2), (36,3), (36,11), (36,33), (37,17), (38,5), (39,2), (39,4), (40,37), (41,2), (42,3), (42,13), (43,2), (43,4), (43,5), (43,8), (43,10), (44,41), (45,2), (45,3), (45,6), (46,43), (47,2), (47,4), (48,3), (48,5), (48,9), (49,2), (52,7), (52,49), (53,2), (53,5), (53,10), (53,25), (53,50), (54,3), (54,17), (55,2), (55,4), (56,53), (57,2), (58,5), (58,11), (58,55), (59,2), (60,3), (60,19), (60,57), (61,2), (61,29), (61,58), (62,59), (63,2), (63,4), (64,61), (66,3), (66,7), (66,9), (66,21), (66,63), (67,2), (67,4), (68,5), (68,13), (68,65), (69,2), (69,3), (69,6), (69,11), (69,22), (69,33), (69,66), (70,67), (71,2), (71,4), (71,17), (71,34), (72,3), (72,23), (72,69), (75,2), (76,73), (77,2), (77,37), (77,74), (78,3), (78,5), (78,25), (79,2), (79,4), (79,19), (79,38), (79,76), (80,7), (80,11), (80,77), (81,2), (81,3), (81,6), (81,13), (81,26), (83,2), (84,3), (84,9), (84,27), (84,81), (85,2), (85,41), (85,82), (86,83), (87,2), (87,4), (88,5), (88,17), (89,2), (90,3), (90,29), (91,2), (92,89), (93,2), (93,3), (93,5), (93,6), (93,9), (93,10), (93,18), (94,7), (94,13), (95,2), (95,4), (96,3), (97,2), (98,5), (98,19), (100,97)

REFERENCES

1. Thomas Beth, Dieter Jungnickel, and Hanfried Lenz, *Design theory. Vol. I*, second ed., Encyclopedia of Mathematics and its Applications, vol. 69, Cambridge University Press, Cambridge, 1999. MR 1729456 (2000h:05019)
2. Bradley W. Brock, *Hermitian congruence and the existence and completion of generalized Hadamard matrices*, J. Combin. Theory Ser. A **49** (1988), no. 2, 233–261. MR 964386 (90a:05038)
3. Yeow Meng Chee, Yin Tan, and Yue Zhou, *Almost p-ary perfect sequences*, Sequences and their applications—SETA 2010, Lecture Notes in Comput. Sci., vol. 6338, Springer, Berlin, 2010, pp. 399–415. MR 2830737 (2012k:94116)
4. Solomon W. Golomb and Guang Gong, *Signal design for good correlation*, Cambridge University Press, Cambridge, 2005, For wireless communication, cryptography, and radar. MR 2156522 (2006d:94021)
5. Tsit Yuen Lam and Ka Hin Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109. MR 1736695 (2001f:11135)
6. Siu Lun Ma and Wei Shean Ng, *On non-existence of perfect and nearly perfect sequences*, Int. J. Inf. Coding Theory **1** (2009), no. 1, 15–38. MR 2747646 (2012a:94140)
7. Ferruh Özbudak, Oğuz Yayla, and C. Cengiz Yıldırım, *Nonexistence of certain almost p-ary perfect sequences*, Sequences and their applications—SETA 2012, Lecture Notes in Comput. Sci., vol. 7280, Springer, Heidelberg, 2012, pp. 13–24. MR 3015455
8. Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)
9. Arne Winterhof, *On the non-existence of generalized Hadamard matrices*, J. Statist. Plann. Inference **84** (2000), no. 1-2, 337–342. MR 1747512 (2000k:05058)

(Arne Winterhof, Oğuz Yayla, Volker Ziegler) JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS (RICAM), AUSTRIAN ACADEMY OF SCIENCES, ALTENBERGERSTR. 69, 4040 LINZ, AUSTRIA

E-mail address: arne.winterhof@ricam.oeaw.ac.at

E-mail address: oguz.yayla@ricam.oeaw.ac.at

E-mail address: volker.ziegler@ricam.oeaw.ac.at