Designs, Codes and Cryptography (2019) 87:2537–2551
https://doi.org/10.1007/s10623-019-00636-7

Hamming correlation properties of the array structure of Sidelnikov sequences

Min Kyu Song[1] · **Hong-Yeop Song**[1]

Received: 31 August 2018 / Revised: 7 April 2019 / Accepted: 16 April 2019 / Published online: 27 April 2019

Abstract
In this paper, we investigate the Hamming correlation properties of column sequences from the $(q-1) \times \frac{q^d-1}{q-1}$ array structure of M-ary Sidelnikov sequences of period q^d-1 for $M|q-1$ and $d \geq 2$. We prove that the proposed set $\Gamma(d)$ of some column sequences has the maximum non-trivial Hamming correlation upper bounded by the minimum of $\frac{q-1}{M}d-1$ and $\frac{M-1}{M}\left[(2d-1)\sqrt{q}+1\right]+\frac{q-1}{M}$. When $M=q-1$, we show that $\Gamma(d)$ is optimal with respect to the Singleton bound. The set $\Gamma(d)$ can be extended to a much larger set $\Delta(d)$ by involving all the constant additions of the members of $\Gamma(d)$, which is also optimal with respect to the Singleton bound when $M=q-1$.

Keywords Codes for FHMA · Sequences · Hamming correlation · Sidelnikov sequences · Array structure

Mathematics Subject Classification 94A05 · 94A55

1 Introduction

Frequency-hopping sequences have been widely used in modern communication systems to resist signal jamming (frequency-hopping spread spectrum, FHSS) or to serve many users at the same time (frequency-hopping multiple access, FHMA) in both military and commercial communication systems [13,24]. For these systems, the receiver can suffer from the interference caused by using the same frequency in the same time (in general, it is called a hit). These are modeled by Hamming auto-correlation for a single sequence or Hamming cross-correlation for a family of sequences. It may be desirable to make the size of frequency-

Communicated by M. Paterson.

✉ Hong-Yeop Song
hysong@yonsei.ac.kr

Min Kyu Song
mk.song@yonsei.ac.kr

[1] School of Electrical and Electronic Engineering, Yonsei University, Yonsei-rho 50, Seoul, Korea

hopping sequence families as large as possible while maintaining low maximum Hamming auto- and cross-correlation [18,19].

In any design of frequency-hopping sequence family, one hit in either Hamming auto-correlation or Hamming cross-correlation is inescapable, and some interesting families in the beginning had been designed with at most one hit. These are summarized in the famous paper by Shaar and Davis in 1984 [22]. From then on, many researchers found optimal frequency-hopping sequence families [1,3,7–9,17,27–29] with respect to the Lempel-Greenberger bound [18], and optimal families [2,4–6,9] with respect to the Peng-Fan bound [19]. Recently, [10] introduced near-optimal frequency hopping sequences with respect to the Lempel-Greenberger bound.

For the perspective of coding theory, the family of frequency-hopping sequences is equivalent to non-binary cyclic codes with good Hamming distance. The earliest example using this is from Reed-Solomon (RS) codes [20]. Some interesting bounds from this relation are obtained [6]. It is interesting to find that the third construction of Reference [6] was founded by Reference [25], based on a well-known property of cyclic codes.

Sidelnikov introduced a sequence over the integers mod M which is now called the Sidelnikov sequence [23]. He proved two different properties of the sequences: (1) the (complex) correlation property and (2) the Hamming correlation property. We call these the first and the second result of Sidelnikov.

The first result of Sidelnikov was extended for constructing sequence families with good (complex) correlation [11,14,15]. Recently, it has been further extended by considering column sequences of the $(q-1) \times \frac{q^d-1}{q-1}$ array structure of a Sidelnikov sequence of period q^d-1. It was initially started by Yu and Gong [30] for the case $d=2$ and generalized by Reference [16] to $d \geq 3$. Later, Kim, Kim, Song analyzed the (complex) correlation of column sequences from the array structure of Sidelnikov sequences of different periods [26].

The second result of Sidelnikov [23, Theorem 4] can be rephrased as follows: for $M|q-1$, the maximum out-of-phase Hamming auto-correlation of an M-ary Sidelnikov sequence of period $q-1$ is $(q-1)/M+i$ where $i \in \{0, 1\}$ depends on q and M. Several decades later, by [12], it was recognized that an optimal frequency-hopping sequence family [4, Theorem 4], constructed separately from Sidelnikov sequences, is indeed a set of a Sidelnikov sequence and all its constant additions. One interesting point is that [23, Theorem 6] implies some special case of [4, Theorem 4]. Now, in this paper, we investigate the Hamming correlation properties of column sequences from the array structure of the Sidelnikov sequences.

After reviewing Sidelnikov sequences and their array structure in Sect. 2, we discuss the Hamming correlation properties of column sequences from the $(q-1) \times \frac{q^d-1}{q-1}$ array structure of M-ary Sidelnikov sequences of period q^d-1 for $M|q-1$ and $d \geq 2$. We prove that the proposed set $\Gamma(d)$ of some column sequences has the maximum non-trivial Hamming correlation upper bounded by the minimum of $\frac{q-1}{M}d-1$ and $\frac{M-1}{M}\left[(2d-1)\sqrt{q}+1\right]+\frac{q-1}{M}$. When $M=q-1$, we show that $\Gamma(d)$ is optimal with respect to the Singleton bound. The set $\Gamma(d)$ can be extended to much larger set $\Delta(d)$ by involving all the constant additions of the members of $\Gamma(d)$, which is also optimal with respect to the Singleton bound when $M=q-1$. In Sect. 4, we finish this paper with two problems for the future work.

2 Preliminaries

2.1 Notation

We will use the following notation:

- p is a prime number.
- q is a prime power $q = p^r$ with a positive integer r.
- $GF(q)$ is the finite field with q elements and $GF(q)^* = GF(q)\backslash\{0\}$.
- α is a primitive element of $GF(q^d)$.
- $\beta = \alpha^{\frac{q^d-1}{q-1}}$ is a primitive element of $GF(q)$.
- $\log_\beta(\cdot)$ is a discrete logarithm from $GF(q)$ to the integers mod $q-1$ defined by

$$\log_\beta(x) = k \quad \text{if} \quad x = \beta^k \in GF(q).$$

  We will use $\log_\beta(0) = 0$ for convenience.
- $p_l(x)$ is the minimal polynomial over $GF(q)$ of $-\alpha^{-l}$.
- $\omega_M = \exp\left(\frac{2\pi\sqrt{-1}}{M}\right)$ is a complex primitive M-th root of unity.
- ψ is a multiplicative character of $GF(q)$ of order M defined by

$$\psi(x) = \omega_M^{\log_\beta(x)}.$$

  Note that $\psi(0) = 1$.

2.2 Correlation of sequences

Throughout this paper, we will analyze the Hamming correlation of sequences that are defined over the integers mod M. We will refer the sequences defined over the integers mod M to M-ary sequences.

Let $x = \{x(t)\}_{t=0}^{L-1}$ and $y = \{y(t)\}_{t=0}^{L-1}$ be two M-ary sequences of period L. The periodic Hamming correlation between x and y at time shift τ is defined by

$$H_{x,y}(\tau) = \sum_{t=0}^{L-1} h\left[x(t+\tau), y(t)\right],$$

where

$$h[a,b] = \begin{cases} 1, & \text{if } a \equiv b \pmod{M} \\ 0, & \text{otherwise.} \end{cases}$$

The Hamming correlation can also be written by using the complex primitive M-th root of unity ω_M as

$$H_{x,y}(\tau) = \sum_{t=0}^{L-1} \left(\frac{1}{M} \sum_{k=0}^{M-1} \omega_M^{(x(t+\tau)-y(t))k} \right). \tag{1}$$

If x, y are the same or y is a cyclic shift of x, then we call it Hamming auto-correlation of x. Otherwise, we call it Hamming cross-correlation of x and y.

Let $\mathscr{K}$ be a set of M-ary sequences of the same period. The maximum non-trivial Hamming correlation among sequences in $\mathscr{K}$, denoted by $H_{\max}(\mathscr{K})$ is

$$H_{\max}(\mathscr{K}) = \max\left\{ \max_{\substack{x\in\mathscr{K}\\ \tau\neq 0}} H_x(\tau), \max_{\substack{x,y\in\mathscr{K}\\ x\neq y}} H_{x,y}(\tau) \right\}.$$

We also need the periodic (complex) correlation between two M-ary sequences x and y of period L at time shift τ, defined by

$$C_{x,y}(\tau) = \sum_{t=0}^{L-1} \omega_M^{x(t+\tau)-y(t)}.$$

Similar to the case of Hamming correlation, for a given set $\mathscr{K}$ of M-ary sequences of the same period, the maximum non-trivial (complex) correlation among sequences in $\mathscr{K}$, denoted by $C_{\max}(\mathscr{K})$, is

$$C_{\max}(\mathscr{K}) = \max\left\{ \max_{\substack{x\in\mathscr{K}\\ \tau\neq 0}} |C_x(\tau)|, \max_{\substack{x,y\in\mathscr{K}\\ x\neq y}} |C_{x,y}(\tau)| \right\}.$$

2.3 Sidelnikov sequences and their array structure

Definition 1 [23,30] For an odd prime power q and an integer d, let α be a primitive element of $GF(q^d)$ and $M \geq 2$ be a divisor of $q^d - 1$. Define, for $k = 0, 1, ..., M-1$,

$$D_k = \left\{ \alpha^{Mi+k} - 1 \mid 0 \leq i < \frac{q^d-1}{M} \right\}.$$

Then, an M-ary Sidelnikov sequence $\{s_d(t)\}$ of period $q^d - 1$ is defined as Reference [23], for $t = 0, 1, ..., q^d - 2$,

$$s_d(t) = \begin{cases} 0, & \text{if } \alpha^t = -1, \\ k, & \text{if } \alpha^t \in D_k, \end{cases}$$

or equivalently [30],

$$s_d(t) = \log_\alpha(\alpha^t + 1) \pmod{M}, \tag{2}$$

with the convention $\log_\alpha(0) = 0$.

Example 1 For $q = 7$ and $d = 2$, a root α of the primitive polynomial $x^2 + x + 3$ over $GF(7)$ is a primitive element of $GF(7^2)$. Then, by (2), a Sidelnikov sequence $\{s_d(t)\}_{t=0}^{7^2-2}$ of period $7^2 - 1 = 48$ can be obtained by letting $s_d(t) = \log_\alpha(\alpha^t + 1) \pmod{M}$ for some non-trivial divisor M of $q^d - 1$. For example, when $M = 6$, a 6-ary Sidelnikov sequence of period 48 is obtained [30]

$$\{s_d(t)\}_{t=0}^{47} = \{4, 1, 5, 0, 5, 1, 5, 1, 2, 4, 4, 2, 2, 2, 5, 4, 2, 4, 3, 3, 1, 0, 4, 4,$$
$$0, 5, 0, 3, 5, 2, 3, 5, 4, 1, 3, 1, 2, 3, 0, 1, 0, 0, 5, 2, 1, 3, 3, 0\}.$$

Furthermore, it was shown by Reference [16] that, when M is also a divisor of $q - 1$, (2) can be written as

$$s_d(t) \equiv \log_\beta\left(N_1^d(\alpha^t + 1)\right) \pmod{M}, \tag{3}$$

where $N_1^d(\cdot)$ is the norm from $GF(q^d)$ to $GF(q)$, and $\beta = \alpha^{\frac{q^d-1}{q-1}}$ is the primitive element of $GF(q)$.

It is always possible to write an M-ary Sidelnikov sequence of period $q^d - 1$ as an array of size $(q-1) \times \frac{q^d-1}{q-1}$. For example, the 6-ary Sidelnikov sequence of period 48 in the above example can be written as a 6×8 array [30]

$$\begin{pmatrix} 4 & 1 & 5 & 0 & 5 & 1 & 5 & 1 \\ 2 & 4 & 4 & 2 & 2 & 2 & 5 & 4 \\ 2 & 4 & 3 & 3 & 1 & 0 & 4 & 4 \\ 0 & 5 & 0 & 3 & 5 & 2 & 3 & 5 \\ 4 & 1 & 3 & 1 & 2 & 3 & 0 & 1 \\ 0 & 0 & 5 & 2 & 1 & 3 & 3 & 0 \end{pmatrix}.$$

In $(q-1) \times \frac{q^d-1}{q-1}$ array of an M-ary Sidelnikov sequence of period $q^d - 1$, the l-th column sequence $v_l(t)$ of the array can be written as [16]

$$v_l(t) = s_d\left(\frac{q^d-1}{q-1}t + l\right), \tag{4}$$

for $t = 0, 1, ..., q-2$.

For a given integer l, denote by $\hat{C}_l(d)$ the q-cyclotmic coset mod $\frac{q^d-1}{q-1}$ which is defined by

$$\hat{C}_l(d) = \left\{l, lq, lq^2, ...\right\},$$

and let m_l be the cardinality of $\hat{C}_l(d)$. Then, m_l is the least positive integer such that [16]

$$\frac{q^d-1}{(q^{m_l}-1)\gcd(\frac{d}{m_l}, q-1)} \Big| l. \tag{5}$$

For a given M-ary Sidelnikov sequence $\{s_d(t)\}$ of period $q^d - 1$, consider its $(q-1) \times \frac{q^d-1}{q-1}$ array structure. Then its column sequences have the following properties [16, Theorem 3 and Corollary 1]:

1. The first column $\{v_0(t)\}$ is a d-multiple of the Sidelnikov sequence of period $q-1$ generated by the primitive element $\beta = \alpha^{\frac{q^d-1}{q-1}}$ of $GF(q)$. That is, for $t = 0, 1, 2, ...q-2$,
$$v_0(t) \equiv d \log_\beta(\beta^t + 1) \pmod{M}.$$
2. If l_1, l_2 are in the same q-cyclotomic coset mod $\frac{q^d-1}{q-1}$, then $\left\{v_{l_1}(t)\right\}$ and $\left\{v_{l_2}(t)\right\}$ are cyclically equivalent, i.e., $\left\{v_{l_2}(t)\right\}$ is a cyclic shift of $\left\{v_{l_1}(t)\right\}$.
3. If $m_l = d$, then the l-th column sequence $\{v_l(t)\}$ does not have any sub-period dividing $q-1$. In fact, it has the full period $q-1$.

We use the following notation originally defined in Reference [16]: $\Lambda(d)$ is the set of smallest representatives of all the q-cyclotomic cosets $\hat{C}_l(d)$ mod $\frac{q^d-1}{q-1}$ except for $l = 0$, and

$$\Lambda'(d) = \{l \in \Lambda(d) | m_l = d\}. \tag{6}$$

[16] gave constructions for sequence families having good (complex) correlation properties by using different subsets of $\Lambda(d)$. Here, we will review briefly only the case with $\Lambda'(d)$. The following results will be used in the remaining of this paper, especially in the discussion

of main contribution of constructing the frequency-hopping sequence families having good Hamming correlation properties.

- The size of $\Lambda'(d)$ is known to be $\lfloor q/2 \rfloor$ for $d = 2$ [30].
- The size of $\Lambda'(d)$ is known for some other cases of d: a prime, a prime power, or a product of two distinct primes [16]. It was proved also by Reference [16] that, for $d \geq 3$, as $q \to \infty$,

$$\left|\Lambda'(d)\right| \sim \frac{q^{d-1}}{d}. \tag{7}$$

- A column sequence $\{v_l(t)\}$ with $l \in \Lambda'(d)$ can be represented by [16]

$$v_l(t) = \log_\beta \left(\beta^l p_l\left(\beta^t\right)\right), \tag{8}$$

where $\beta = \alpha^{\frac{q^d-1}{q-1}}$ is primitive in $GF(q)$ and $p_l(x)$ is the minimal polynomial of degree d over $GF(q)$ of $-\alpha^{-l}$.

- For a prime power q, let d be an integer with $d \geq 2$, $M \geq 2$ be a divisor of $q^d - 1$, and $\{s_d(t)\}$ be a Sidelnikov sequence of period $q^d - 1$. Define a set of column sequences $\Sigma'(d)$ by

$$\Sigma'(d) = \left\{c v_l(t) | l \in \Lambda'(d), 1 \leq c < M\right\}. \tag{9}$$

Then, the set $\Sigma'(d)$ has following properties [16, Theorems 4, 6]:

1. All the sequences in $\Sigma'(d)$ are cyclically distinct when $2 \leq d < \frac{1}{2}(\sqrt{q} - \frac{2}{\sqrt{q}} + 1)$.
2. The size of $\Sigma'(d)$ is asymptotic to $\frac{(M-1)q^{d-1}}{d}$ as $q \to \infty$.
3. $C_{\max}(\Sigma'(d))$ is upper-bounded as

$$C_{\max}(\Sigma'(d)) \leq (2d-1)\sqrt{q} + 1. \tag{10}$$

3 Main construction for sequences with good Hamming correlation properties

Definition 2 Let $M \geq 2$ be a divisor of $q - 1$ and $d \geq 2$. Consider an M-ary Sidelnikov sequence of period $q^d - 1$ given in (2) or (3), its $(q-1) \times \frac{q^d-1}{q-1}$ array structure and its column sequences given in (4) or (8). Define $\Gamma(d)$ to be the set of its column sequences indexed by $\Lambda'(d)$ in (6), that is,

$$\Gamma(d) = \left\{v_l(t) | l \in \Lambda'(d)\right\}. \tag{11}$$

Theorem 1 *(*Hamming correlation bound of $\Gamma(d)$*) For the sequences in $\Gamma(d)$ of Definition 2,*

$$H_{\max}(\Gamma(d)) \leq \min\left\{\frac{(q-1)d}{M} - 1, \quad \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q} + 1]\right\}. \tag{12}$$

Proof From (8), we have

$$\omega_M^{v_l(t)} = \omega_M^{\log_\beta(\beta^l p_l(\beta^t))} = \psi(\beta^l p_l(\beta^t)).$$

Therefore, by using (1), the Hamming correlation of two column sequences $v_{l_1}(t)$ and $v_{l_2}(t)$ of the $(q-1) \times \frac{q^d-1}{q-1}$ array structure of a Sidelnikov sequence of length $q^d - 1$ with column indices $l_1, l_2 \in \Lambda'(d)$ can be written as

$$H_{l_1,l_2}(\tau) = \sum_{t=0}^{q-2} \frac{1}{M} \sum_{k=0}^{M-1} (\omega_M^{v_{l_1}(t+\tau)})^k (\omega_M^{v_{l_2}(t)})^{-k} \tag{13}$$

$$= \sum_{t=0}^{q-2} \frac{1}{M} \sum_{k=0}^{M-1} [\psi(\beta^{l_1} p_{l_1}(\beta^{t+\tau}))]^k [\psi(\beta^{l_2} p_{l_2}(\beta^t))]^{-k}. \tag{14}$$

Note that $\psi(x)$ is multiplicative over $GF(q)^*$ and $\beta^l p_l(\beta^t) \neq 0$ for any t since $p_l(x)$ is the minimal polynomial of degree $d \geq 2$ over $GF(q)$. Thus, (14) becomes

$$H_{l_1,l_2}(\tau) = \sum_{t=0}^{q-2} \frac{1}{M} \sum_{k=0}^{M-1} \psi^k(\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1}). \tag{15}$$

We now focus on the inner summation of the above, especially on the argument of ψ^k. Note that

$$\frac{1}{M} \sum_{k=0}^{M-1} \psi^k(x) = \begin{cases} 1, & \text{if } x = 0, \\ 1, & \text{if } x = (\beta^M)^e \text{ for some } e \in \left\{0, 1, ..., \frac{q-1}{M} - 1\right\}, \\ 0, & \text{otherwise.} \end{cases} \tag{16}$$

Since $p_{l_1}(x)$ and $p_{l_2}(x)$ are minimal polynomials of the same degree $d \geq 2$, the expression $\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1}$ becomes nonzero for any l_1, l_2, τ, and t. Thus, we should count the number of elements β^t in $GF(q)^*$ such that

$$\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1} = \beta^{eM}, \tag{17}$$

for some $e \in \left\{0, 1, 2, ..., \frac{q-1}{M} - 1\right\}$, as t runs from 0 to $q-2$. For any β^t which satisfies (17) with some appropriate e, the above relation (17) implies

$$[\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau}) p_{l_2}(\beta^t)^{-1}]^{(q-1)/M} = (\beta^{eM})^{(q-1)/M} = 1,$$

or

$$[\beta^{l_1-l_2} p_{l_1}(\beta^{t+\tau})]^{(q-1)/M} - [p_{l_2}(\beta^t)]^{(q-1)/M} = 0. \tag{18}$$

Now, we let

$$g(x) = [\beta^{l_1-l_2} p_{l_1}(\beta^\tau x)]^{(q-1)/M} - [p_{l_2}(x)]^{(q-1)/M}.$$

Then, $H_{l_1,l_2}(\tau)$ is the number of roots of $g(x)$ in $GF(q)^*$.

If $l_1 = l_2$ and $\tau = 0 \mod q-1$, the polynomial $g(x)$ becomes identically zero, and every member of $GF(q)^*$ is a root. Therefore,

$$H_{l_1,l_2}(\tau) = H_{l_1,l_1}(0) = q - 1.$$

Otherwise, we consider the case where either $l_1 \neq l_2$ or $\tau \neq 0 \mod q-1$. In this case, $g(x)$ cannot be identically zero, and hence, $g(x)$ is a non-zero polynomial of degree at most $\frac{q-1}{M} d$. Since $p_l(x)$ is the minimal polynomial of $-\alpha^{-l}$, its constant term becomes $(-1)^d N_1^d(-\alpha^{-l}) = \beta^{-l}$. Thus, the constant term of $g(x)$ becomes 0, since

$$[\beta^{l_1-l_2} \beta^{-l_1}]^{(q-1)/M} - (\beta^{-l_2})^{(q-1)/M} = 0.$$

This implies that $g(x) = xf(x)$ for some polynomial $f(x)$ of degree at most $\frac{q-1}{M} d - 1$ over $GF(q)$. Therefore, we obtain the bound,

$$H_{\max}(\Gamma(d)) \leq \frac{q-1}{M} d - 1. \tag{19}$$

On the other hand, from (13), we can obtain another bound by using (10):

$$\begin{aligned} H_{l_1,l_2}(\tau) &= \frac{1}{M}\sum_{k=0}^{M-1}\sum_{t=0}^{q-2}(\omega_M^{v_{l_1}(t+\tau)})^k(\omega_M^{v_{l_2}(t)})^{-k} \\ &\le \frac{q-1}{M} + \frac{1}{M}\sum_{k=1}^{M-1}\left|\sum_{t=0}^{q-2}(\omega_M^{v_{l_1}(t+\tau)})^k(\omega_M^{v_{l_2}(t)})^{-k}\right| \\ &\le \frac{q-1}{M} + \frac{M-1}{M}C_{\max}(\Gamma(d)) \\ &\le \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]. \end{aligned} \tag{20}$$

By taking the minimum of the two bounds in (19) and (20), we obtain (12). □

Remark 1 The following are some remarks on the upper-bound in (12).

1. One special case happens when $q > 3$ and $M = q-1$. In this case, we have
$$H_{\max}(\Gamma(d)) \le d-1. \tag{21}$$
Furthermore, the very special case is $H_{\max}(\Gamma(2)) \le 1$. Such a frequency-hopping sequence family was named 'one-coincidence sequences' by Shaar and Davis and is known to be optimal [22].
2. The other extreme case is when q is odd and $M = 2$. In this case, we have
$$H_{\max}(\Gamma(d)) \le \frac{q-1}{2} + \frac{1}{2}[(2d-1)\sqrt{q}+1]$$
for d with $2 \le d < \frac{1}{2}(\sqrt{q} - 2/\sqrt{q}+1)$.
3. Let the two bounds in (19) and (20) be denoted by B_1 and B_2, respectively. For given q and d, we can find M such that
$$B_1 = \frac{q-1}{M}d - 1 = \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1] = B_2.$$
It turns out that
$$M_0 = \frac{(q-1)(d-1)-1}{(2d-1)\sqrt{q}+2} + 1$$
is the solution, and, since M is an integer, we may conclude that
$$B_1 > B_2 \quad \text{if and only if} \quad M > M_0.$$
For $q = 101$ and $d = 2$, Table 1 shows B_1 and B_2, and minimum of them. Here, observe that B_1 is greater than B_2 when $M \le 4 < M_0 = 4.08$.

Table 2 shows the true maximum of non-trivial Hamming auto- and cross-correlation for q=101, $d = 2, 3$, and all possible values of M. From this, we can observe that the true maximum meets (12) when $M \ge 10 = \sqrt{q-1}$ for $d = 2$ and $M \ge 20 = 2\sqrt{q-1}$ for $d = 3$.

Corollary 1 *For a positive integer c such that* $\gcd(c, M) = 1$, *define*

$$c\Gamma(d) = \{cv_l(t) | v_l(t) \in \Gamma(d)\}.$$

The maximum non-trivial Hamming correlation of $c\Gamma(d)$ is also upper-bounded by (12).

Table 1 Behavior of the bound in (12) for $q = 101$, $d = 2$, and various M

M	$B_1 = \frac{q-1}{M}d - 1$	$B_2 = \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q}+1]$	$\min(B_1, B_2)$
100	1	31	1
50	3	32	3
25	7	33	7
20	9	34	9
10	19	38	19
5	39	44	39
4	49	48	48
2	99	65	65

Table 2 Maximum Hamming correlation values and bound in (12) for $q = 101$ and various M, d

M	$d = 2, \lvert\Gamma(d)\rvert = 50$			$d = 3, \lvert\Gamma(d)\rvert = 3434$		
	$H_{a,\max}$	$H_{c,\max}$	Bound (12)	$H_{a,\max}$	$H_{c,\max}$	Bound (12)
100	1	1	1	2	2	2
50	3	3	3	5	5	5
25	7	7	7	11	11	11
20	9	9	9	14	14	14
10	18	19	19	25	25	29
5	32	33	39	38	39	59
4	36	37	48	46	46	63
2	58	59	65	68	69	75

Proof Since $(c, M) = 1$, we have $\omega_M^{cv_l(t)} = (\omega'_M)^{v_l(t)}$, where ω'_M is another primitive M-th root of unity. That is, the constant c just changes ω_M to ω'_M. □

From the definition of $\Gamma(d)$, it is obvious that $|\Gamma(d)| = |\Lambda'(d)|$. As mentioned at the end of Sect. 2, it was known by Reference [16] that $\left|\Lambda'(d)\right| \sim \frac{q^{d-1}}{d}$ for $d \geq 3$. And, we observe that it is indeed a lower bound:

Lemma 1 *Let $3 \leq d \leq M$. The size of column index set $\Lambda'(d)$ is lower bounded by q^{d-1}/d.*

Proof The proof is given in Appendix. □

Now, we will show that, when $M = q - 1$ and $2 \leq d \leq q - 1$, the proposed frequency-hopping sequence family $\Gamma(d)$ is optimal with respect to the Singleton bound:

Lemma 2 *(Singleton bound for frequency-hopping sequences* [21, Equation (18)]*) Let $\mathscr{K}$ be a family of N frequency-hopping sequences of length L over an alphabet of size M. Then,*

$$H_{\max}(\mathscr{K}) \geq \lceil \log_M(NL) - 1 \rceil,$$

where $\log_M(\cdot)$ is the logarithm to the base M over the reals.

Theorem 2 *Let $M = q - 1$ and $2 \leq d \leq q - 1$. Then the frequency-hopping sequence family $\Gamma(d)$ in Definition 2 is optimal with respect to the Singleton bound.*

Proof From Lemma 2, we have following lower bound on $H_{\max}(\Gamma(d))$:

For $d = 2$, we have $N = \lfloor \frac{q}{2} \rfloor$ and $L = q - 1$. Therefore,

$$\begin{aligned} H_{\max}(\Gamma(2)) &\geq \lceil \log_{q-1}(\lfloor \frac{q}{2} \rfloor (q-1)) - 1 \rceil \\ &\geq \lceil 1 - \log_{q-1} 2 \rceil = 1. \end{aligned}$$

For $d \geq 3$, we have $N \geq \frac{q^{d-1}}{d}$ and $L = q - 1$. Therefore,

$$\begin{aligned} H_{\max}(\Gamma(d)) &\geq \lceil \log_{q-1}(\frac{(q-1)q^{d-1}}{d}) - 1 \rceil \\ &\geq \lceil d - 1 - \log_{q-1} d \rceil = d - 1. \end{aligned}$$

From (12) and (21), we conclude that $\Gamma(d)$ is optimal with respect to the Singleton bound for $M = q - 1$ and $2 \leq d \leq q - 1$. □

Remark 2 The above can be described alternatively by using the k-th order near-orthogonal codes from RS codes [20,25]. For each $l \in \Lambda'(d)$, the function $\log_\beta(\beta^l p_l(\beta^t))$ generates the l-th column sequence and the polynomial $\beta^l p_l(\beta^t)$ of degree d generates a sequence of length $q - 1$ over $GF(q)$, which corresponds to a codeword of a q-ary RS code of length $q-1$. The corresponding codeword has no zero element, since the polynomial is minimal and is of degree $d \geq 2$. From the Hamming distance property of RS codes, it is obvious that all the codewords corresponding to a minimal polynomial of degree d are Hamming-correlated at most $d - 1$ from each other. Since there is no 0, the map $\log_\beta(\cdot)$ does not affect on the Hamming correlation.

Remark 3 With the same notations as in Lemma 2, The Peng-Fan bound [19] says that

$$H_{\max}(\mathscr{K}) \geq \frac{(LN - M)L}{(LN - 1)M}.$$

The family $\Gamma(d)$ becomes optimal when $d = 2$ and not optimal otherwise, with respect to the Peng-Fan bound above.

For $d = 2$, Yu and Gong [30] formalized the l-th column sequence as

$$v_l(t) = \log_\beta(\beta^{(q+1)t+l} + \mathrm{Tr}_1^2(\alpha^{(q+1)t+l}) + 1),$$

where $\mathrm{Tr}_b^a(x)$ is the trace from $GF(q^a)$ to $GF(q^b)$. By using this, $p_l(x)$ in (8) becomes

$$p_l(x) = x^2 + \mathrm{Tr}_1^2(\alpha^{-l})x + \mathrm{N}_1^2(\alpha^{-l}). \tag{22}$$

Corollary 2 *If $M = q - 1$, then the sequence $v_l(t) \in \Gamma(2)$ has one of the following Hamming auto-correlation profiles:*

1. *If q is even, then*

$$H_l(\tau) = \begin{cases} q - 1, & \text{if } \tau = 0 \mod q - 1 \\ 1, & \text{otherwise.} \end{cases}$$

2. *If q is odd, then*

$$H_l(\tau) = \begin{cases} q - 1, & \text{if } \tau = 0 \mod q - 1 \\ 0, & \text{if } \tau = \frac{q-1}{2} \mod q - 1 \\ 1, & \text{otherwise.} \end{cases}$$

Proof From (22),

$$p_l(\beta^{t+\tau}) - p_l(\beta^t) = [\beta^{2t+2\tau} + \mathrm{Tr}_1^2(\alpha^{-l})\beta^{t+\tau} + \mathrm{N}_1^2(\alpha^{-l})] - [\beta^{2t} + \mathrm{Tr}_1^2(\alpha^{-l})\beta^t + \mathrm{N}_1^2(\alpha^{-l})]$$
$$= \beta^t[\beta^t(\beta^{2\tau} - 1) - \mathrm{Tr}_1^2(\alpha^{-l})(\beta^\tau - 1)].$$

Note that the condition of $\mathrm{Tr}_1^2(\alpha^{-l}) = 0$ is

$$\mathrm{Tr}_1^2(\alpha^{-l}) = 0$$
$$\Leftrightarrow \alpha^{-l} + \alpha^{-ql} = 0$$
$$\Leftrightarrow 1 + \alpha^{-(q-1)l} = 0.$$

If q is even, $\mathrm{Tr}_1^2(\alpha^{-l})$ can not be 0 for all $l \in \Lambda'(d)$. If q is odd, $\mathrm{Tr}_1^2(\alpha^{-l}) = 0$ when $l = \frac{q+1}{2}$ mod $q-1$, which are not in $\Lambda'(d)$. Thus, $\mathrm{Tr}_1^2(\alpha^{-l}) \neq 0$ for any $l \in \Lambda$. Let $\tau \neq 0 \mod q-1$. Then, $\beta^\tau - 1 \neq 0$. If q is even, $1 - \beta^{2\tau}$ is non-zero for any $\tau \neq 0 \mod q-1$. So, it always has a root. If q is odd, $\beta^{2\tau} - 1$ will be zero when $\tau = \frac{q-1}{2} \mod q-1$. For any other $\tau \neq 0$ mod $q-1$, it always has a root. □

The proposed family $\Gamma(d)$ can be enlarged as follows by including all the constant additions of the sequences in it:

Definition 3 Let $M \geq 2$ be a divisor of $q-1$. Let $\Gamma(d)$ be in Definition 2. Define $\Delta(d)$ to be a set of M-ary sequences including $\Gamma(d)$ and all its constant additions, that is,

$$\Delta(d) = \bigcup_{0 \leq c < M} (c + \Gamma(d)) = \{v_l(t) + c | 0 \leq c < M, v_l(t) \in \Gamma(d)\}.$$

Theorem 3 *(Hamming correlation bound of $\Delta(d)$) For the sequences in $\Delta(d)$ of Definition 3,*

$$H_{\max}(\Delta(d)) \leq \min\left\{\frac{(q-1)d}{M}, \frac{q-1}{M} + \frac{M-1}{M}[(2d-1)\sqrt{q} + 1]\right\}. \quad (23)$$

Proof We note that

$$v_l(t) + c = \log_\beta(\beta^{l+c} p_l(\beta^t)) \mod M.$$

Then, the proof is similar to that of Theorem 1. □

Table 3 Maximum non-trivial Hamming correlation values and bound of $\Delta(d)$ for $q = 101$, $d = 2$, and various M

M	$H_{a,max}$	$H_{c,max}$	Upper-bound in (23)	$\lvert\Gamma(d=2)\rvert$	$\lvert\Delta(d=2)\rvert$
100	1	2	2	50	5000
50	3	4	4	50	2500
25	7	8	8	50	1250
20	9	10	10	50	1000
10	18	20	20	50	500
5	32	34	40	50	250
4	36	38	48	50	200
2	58	60	65	50	100

Table 4 Comparison with some known frequency-hopping sequence families

		Length	Alphabet size M	H_{max}	Set size
Sidelnikov (implicit, Theorem 6)	[23]	$q-1$	$M \mid q-1, q$ or $\frac{q-1}{M}$ should be even	$\frac{q-1}{M}+1$	–
Lempel and Greenberger	[18]	p^r-1	$p^u, 0<u\le r$	$p^{r-u}-1$	$M=p^u$
Kumar	[17]	p^2	p	p	p
Song et al.	[25]	$q-1$	q	$1\le k\le B(q)<q-1=n$	$\frac{1}{n}\sum_{d\mid n}\mu(d)q^{1+\lfloor\frac{k}{d}\rfloor}$
Udaya and Siddiqi	[29]	$p^{cn}-1$	$M=p^t$ where $1\le t<n$	$p^{cn-t}-1$	p
Chu and Colbourn	[2]	p	$M=e+1$, where $e\mid p-1$	$\frac{p-1}{e}$	e
Ding, Miosio, and Yuan	[5]	q^n-1	q	q^{n-1}	q
1st of Ding and Yin (corrected by Ref. [12])	[4]	$q-1$	$M\mid q-1$ with $M\ge 2$	$\frac{q-1}{M}$, if q or $\frac{q-1}{M}$ is even $\frac{q-1}{M}+1$, if q and $\frac{q-1}{M}$ is odd	M
Su	[27]	p^2	p	p	p
$\Gamma(d)$ in this paper		$q-1$	$M\mid q-1$ with $M\ge 2$	$\le$ minimum of $\frac{(q-1)d}{M}-1$ and $\frac{q-1}{M}+\frac{M-1}{M}[(2d-1)\sqrt{q}+1]$	$\ge \frac{q^{d-1}}{d}$
$\Delta(d)$ in this paper		$q-1$	$M\mid q-1$ with $M\ge 2$	$\le$ minimum of $\frac{(q-1)d}{M}$ and $\frac{q-1}{M}+\frac{M-1}{M}[(2d-1)\sqrt{q}+1]$	$\ge M\frac{q^{d-1}}{d}$

From the definition of $\Delta(d)$, it is easy to see that $|\Delta(d)| = M\,|\Gamma(d)|$.

Theorem 4 *Let $M = q - 1$ and $2 \le d \le q - 2$. Then, the frequency hopping sequence family $\Delta(d)$ is optimal with respect to the Singleton bound.*

Proof We omit the proof since it is similar to that of Theorem 2. □

Table 3 shows the maximum Hamming auto- and cross-correlation values and the derived bound for $q = 101$, $d = 2$, and all possible values of M. As is the case of $\Gamma(d)$, the exact maximum non-trivial Hamming correlation of $\Delta(d)$ attains the bound in (23) when $M \ge 10 = \sqrt{q-1}$ for $d = 2$.

In Table 4, some well-known frequency-hopping sequence families and the proposed sequence families are presented with their parameters. We note that $\Delta(d)$ is applicable for all prime powers $q > 3$. From Table 4, we see that the family size is larger than the length for $\Gamma(d)$ and $\Delta(d)$ of this paper and also the family in Reference [25]. For all other cases, the family size is smaller than the length. Note that, as discussed in Remark 2, $\Gamma(d)$ and $\Delta(d)$ are closely related to the k-th order near orthogonal codes in Reference [25].

4 Concluding remarks

In this paper, we investigated Hamming correlation properties of some column sequences of length $q - 1$ from the array structure of an M-ary Sidelnikov sequence of period $q^d - 1$, and construct two frequency-hopping sequence families both of them are optimal with respect to the Singleton bound for the case $M = q - 1$. The column sequences are selected by the index set $\Lambda'(d)$. We note that Reference [16] discussed the (complex) correlation properties of the same set by $\Lambda'(d)$, while we discuss the Hamming correlation properties.

Following are two open problems for the future:

1. It would be essential to identify $\Lambda'(d)$ in an efficient manner for practical use since it is difficult to systematically enumerate the members of $\Lambda'(d)$ in general [16]. Find an algorithm which outputs the members of $\Lambda'(d)$ as many as possible systematically.
2. In Table 2, the true maximum non-trivial Hamming correlation value attains the upper-bound $\frac{q-1}{M}d - 1$ for some choices of M. It would be interesting to find an explicit condition on M and other parameters at which the true maximum non-trivial Hamming correlation value attains the upper-bound.

Acknowledgements This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2017R1A2B4011191).

Appendix: Proof of Lemma 1

Recall that $m_l = d$ for any $l \in \Lambda'(d)$ and m_l is the least positive integer which satisfies (5). Then, it is easy to see that

$$\left|\Lambda'(d)\right| = \frac{1}{d}\left(\frac{q^d - 1}{q - 1} - k - 1\right), \tag{24}$$

where

$$k = \sum_{\substack{r|d \\ r\neq 1 \\ r\neq d}} \left| \left\{ l \mid 1 \le l < \frac{q^d-1}{q-1}, m_l = r \right\} \right|. \tag{25}$$

From (5), there are

$$\frac{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)}{q-1}$$

column indices from 1 to $\frac{q^d-1}{q-1}-1$, which can be divided by

$$\frac{q^d-1}{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)},$$

where $2 \le r \le d$. So, we have

$$k < \sum_{\substack{r|d \\ r\neq d \\ r\neq 1}} \frac{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)}{q-1}. \tag{26}$$

Note that any divisor of d is less than or equal to $\lfloor d/2 \rfloor$ and $\gcd\left(\frac{d}{r}, q-1\right) \le q-1$. By using these, observe that

$$k < \sum_{r=2}^{\lfloor d/2 \rfloor} \frac{(q^r-1)\gcd\left(\frac{d}{r}, q-1\right)}{q-1} < \sum_{r=2}^{\lfloor d/2 \rfloor} q^r < \frac{q^{\lfloor d/2 \rfloor+1}-1}{q-1} - 1 \tag{27}$$

By substituting (27) into (24) finally, we obtain the result. □

References

1. Cao Z., Ge G., Miao Y.: Combinatorial characterizations of one-coincidence frequency-hopping sequences. Des. Codes Cryptgr. **41**(2), 177–184 (2006).
2. Chu W., Colbourn C.J.: Optimal frequency-hopping sequences via cyclotomy. IEEE Trans. Inf. Theory **51**(3), 1139–1141 (2005).
3. Chung J.-H., Han Y.K., Yang K.: New classes of optimal frequency-hopping sequences by interleaving techniques. IEEE Trans. Inf. Theory **55**(12), 5783–5791 (2009).
4. Ding C., Yin J.: Sets of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **54**(8), 3741–3745 (2008).
5. Ding C., Miosio M.J., Yuan J.: Algebraic constructions of optimal frequency-hopping sequences. IEEE Trans. Inf. Theory **53**(7), 2606–2610 (2007).
6. Ding C., Fuji-Hara R., Fujiwara Y., Jimbo M., Mishima M.: Sets of frequency hopping sequences: bounds and optimal constructions. IEEE Trans. Inf. Theory **55**(7), 3297–3304 (2009).
7. Fuji-Hara R., Miao Y., Mishima M.: Optimal frequency hopping sequences: a combinatorial approach. IEEE Trans. Inf. Theory **50**(10), 2408–2420 (2004).
8. Ge G., Fuji-Hara R., Miao Y.: Further combinatorial constructions for optimal frequency hopping sequences. J. Comb. Theory **113**, 1699–1718 (2006).
9. Ge G., Miao Y., Yao Z.: Optimal frequency hopping sequences: auto- and cross-correlation properties. IEEE Trans. Inf. Theory **55**(2), 867–879 (2009).
10. Han, Y. K., Yang, K.: New near-optimal frequency-hopping sequences of length pq. Proceedings on 2008 IEEE International Symposium on Information Theory, 2593–2597 (2008).
11. Han Y.K., Yang K.: New M-ary sequence families with low correlation and large size. IEEE Trans. Inf. Theory **55**(4), 1815–1823 (2009).

12. Han Y.K., Yang K.: On the Sidelnikov sequences as frequency-hopping sequences. IEEE Trans. Inf. Theory **55**(9), 4279–4285 (2009).
13. Holmes J.K.: Spread Spectrum Systems for GNSS and Wireless Communications. Artech House, Boston (2007).
14. Kim Y.-J., Song H.-Y.: Cross correlation of Sidelnikov sequences and their constant multiples. IEEE Trans. Inf. Theory **53**(3), 1220–1224 (2007).
15. Kim Y.-S., Chung J.-S., No J.-S., Chung H.: New families of M-ary sequences with low correlation constructed from Sidelnikov sequences. IEEE Trans. Inf. Theory **54**(8), 3768–3774 (2008).
16. Kim Y.-T., Kim D.S., Song H.-Y.: New M-ary Sequence families with low correlation from the array structure of Sidelnikov sequences. IEEE Tans. Inf. Theory **61**(1), 655–670 (2015).
17. Kumar P.V.: Frequency-hopping code sequence designs having large linear span. IEEE Trans. Inf. Theory **34**(1), 146–151 (1988).
18. Lempel A., Greenberger H.: Families of sequences with optimal Hamming correlation properties. IEEE Trans. Inf. Theory **20**(1), 90–94 (1974).
19. Peng D., Fan P.: Lower bounds on the Hamming auto- and cross correlations of frequency-hopping sequences. IEEE Trans. Inf. Theory **50**(9), 2149–2154 (2004).
20. Reed I.: kth-Order near-orthogonal codes. IEEE Trans. Inf. Theory **17**(1), 116–117 (1971).
21. Sarwate D.V.: Reed-Solomon Codes and the Design of Sequences for Spread-Spectrum Multiple-Access Communications. IEEE Press, Piscataway (1994).
22. Shaar A.A., Davis P.A.: A survey of one-coincidence sequences for frequency-hopped spread-spectrum systems. Commun. Radar Signal Process. IEE Proc. F **131**(7), 719–724 (1984).
23. Sidelnikov V.M.: Some k-valued pseudo-random sequences and nearly equidistant codes. Probl. Peredachi Inf. **5**(1), 16–22 (1969).
24. Simon M.K., Omura J.K., Scholtz R.A., Levitt B.K.: Spread Spectrum Communications Handbook. McGraw-Hill, New York (1994).
25. Song H.Y., Reed I.S., Golomb S.W.: On the nonperiodic cyclic equivalence classes of reed-solomon codes. IEEE Trans. Inf. Theory **39**(4), 1431–1434 (1993).
26. Song, M. K., Song. H.-Y.: Correlation properties of sequences from the 2-D array structure of Sidelnikov sequences of different lengths and their union. In the 2016 IEEE International Symposium on Information Theory, pp. 105–108 (2016)
27. Su M.: New optimum frequency hopping sequences derived from fermat quotients. The Sixth International Workshop on Signal Design and Its Applications in Communications **166–169**, (2013).
28. Titlebaum E.L.: Time-frequency hop signals Part I: coding based upon the theory of linear congruences. IEEE Trans. Aerospace Electron. Syst. **AES–17**(4), 490–493 (1981).
29. Udaya P., Siddiqi M.U.: Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings. IEEE Trans. Inf. Theory **44**(4), 1492–1503 (1998).
30. Yu N.Y., Gong G.: New construction of M-ary sequence families with low correlation from the structure of Sidelnikov sequences. IEEE Trans. Inf. Theory **56**(8), 4061–4070 (2010).