A new family of arrays with low autocorrelation

Heiko Dietrich and Nathan Jolly

ABSTRACT. Arrays with low autocorrelation are widely sought in applications; important examples are arrays whose periodic autocorrelation is zero for all nontrivial cyclic shifts, so-called perfect arrays. In 2001, Arasu and de Launey defined almost perfect arrays: these have size $2u \times v$ and autocorrelation arrays with only two nonzero entries, namely $2uv$ and $-2uv$ in positions $(0,0)$ and $(u,0)$, respectively. In this paper we present a new class of arrays with low autocorrelation: for an integer $n \geq 1$, we call an array n-perfect if it has size $nu \times v$ and if its autocorrelation array has only n nonzero entries, namely $nuv\lambda^i$ in position $(iu,0)$ for $i = 0,1,\ldots,n-1$, where λ is a primitive n-th root of unity. Thus, an array is 1-perfect (2-perfect) if and only if it is (almost) perfect. We give examples and describe a recursive construction of families of n-perfect arrays of increasing size.

1. Introduction

An array has *low autocorrelation* if its periodic autocorrelation for most nontrivial cyclic shifts is zero; of particular importance are *perfect arrays* whose periodic autocorrelation is zero for all nontrivial cyclic shifts. Because of this impulse-like behaviour, arrays with low autocorrelation are useful in numerous applications, such as digital watermarking [6, 11, 15, 16, 17], frequency hopping patterns for radar, and sonar communications [10, 13], time hopping patterns for UWB radio [12], and two-dimensional optical orthogonal coding [14].

Perfect arrays are difficult to find, and there has been some focus on other classes of arrays with low autocorrelation. Recall that a $u \times v$ array is perfect if its autocorrelation array is all zeroes except for uv in position $(0,0)$. In 2001, Arasu and de Launey [1] considered a modification: they called a $2u \times v$ array *almost perfect* if its autocorrelation array is all zeroes except for $2uv$ and $-2uv$ in position $(0,0)$ and $(u,0)$, respectively. They proposed a recursive construction yielding almost perfect arrays of arbitrarily large sizes: their method involved concatenating two almost perfect arrays horizontally, column-shifting that concatenation in two possible ways, and then interleaving the rows of these arrays.

The aim of this paper is to present a new class of arrays with low autocorrelation, generalising perfect and almost perfect arrays. Let $n \geq 2$ be an integer and let λ be a complex primitive n-th root of unity. We call an $nu \times v$ array *n-perfect* if the only nonzero entries of its autocorrelation array are $nuv\lambda^i$ in position $(iu,0)$ for $i = 0,1,\ldots,n-1$. It follows from the definition that an array is 1-perfect (2-perfect) if and only if it is (almost) perfect. Motivated by the discussion of almost perfect arrays in [1], our main result here is a recursive construction of n-perfect arrays: Starting with a certain n-perfect array, we concatenate n copies of it side-by-side, then apply n distinct column shifts to these copies, and eventually interleave these arrays to form one large n-perfect array with both horizontal and vertical sizes multiplied by n. This construction can be applied repeatedly to yield arbitrarily large n-perfect arrays over the same alphabet. We provide a variety of n-perfect arrays of size $n^2 \times n$, and each can be used to construct perfect arrays of size $n^{k+1} \times n^k$ for all $k \geq 1$.

1.1. Motivation. The idea to define n-perfect arrays arose during the development of the algebraic framework to work with arrays, in particular, almost perfect arrays (see [4, 5]). There are three main reasons why n-perfect arrays are worth studying. First, the class of n-perfect arrays is very interesting from a mathematical point of view since it covers (and therefore generalises) the important classes of perfect and almost perfect arrays. It is a common theme in mathematics to seek generalisations of successful

SCHOOL OF MATHEMATICAL SCIENCES, MONASH UNIVERSITY, CLAYTON VIC 3800, AUSTRALIA
E-mail addresses: heiko.dietrich@monash.edu, nathanjamesjolly@gmail.com.
Key words and phrases. almost perfect arrays, n-perfect arrays, periodic autocorrelation, recursive constructions.
Most results of this paper are part of the second author's PhD thesis at Monash University, Melbourne, Australia, supervised by Tom Hall, Imants Svalbe, and the first author. Both authors thank Imants Svalbe and Santiago Barrera Acevedo for feedback on previous versions of this draft. The first author was supported by an ARC DECRA (Australia), project DE140100088.
The final publication is available at Springer via http://dx.doi.org/10.1007/s12095-017-0214-0.

concepts; this paper discusses algebraic properties and constructions of n-perfect arrays, and therefore is a first step in that direction. Second, as outlined in the introduction, arrays with low autocorrelation have various important applications in different areas, and new constructions of families of arrays of unbounded sizes with low-peak autocorrelation are sought (see, for instance, [11] for a discussion of this in the context of watermarking). The class of n-perfect arrays introduced in this paper is a *new class* of arrays with these properties, and therefore can be used in all these applications. We stress that the autocorrelation array of an n-perfect array has n nonzero entries with prescribed magnitude and position. While this makes them seem *less perfect* than almost perfect arrays (if one takes the number of nonzero autocorrelation entries as a measure), their autocorrelation arrays have *more structure* than those of almost perfect arrays. This is our third reason motivating the study of n-perfect arrays: This additional structure has the potential to lead to new applications, for example, in the generation of a fingerprint or fiducial marker of sorts, whose multiple correlation spikes might be useful for scale or orientation determination in digital data.

1.2. Structure of the paper. In Section 2 we introduce the necessary preliminaries and notation for manipulating arrays. Our main result and examples are then discussed in Section 3. The correctness of our recursive construction is proved in Section 4. We end with a conclusion in Section 5.

2. An algebra of arrays

In this section we briefly recall the necessary background and notation for describing our new results. Instead of representing arrays as Laurent polynomials (modulo a suitable ideal), as done in [1], we describe our arrays as elements in a certain *matrix algebra*. Formulating proofs and results in terms of an algebra and certain algebra operations makes the exposition not only shorter, but also more structurally concise; see the discussion in [4, 5].

Definition 2.1. A $u \times v$ *array* is a complex $u \times v$ matrix A with entries $A[i, j]$ where $i \in \{0, \ldots, u-1\}$ and $j \in \{0, \ldots, v-1\}$. If $s, t \in \mathbb{Z}$, then we define

$$A[s, t] = A[s \bmod u, t \bmod v].$$

Component-wise scalar multiplication and addition furnish the set $\mathbb{M}_{u,v}(\mathbb{C})$ of all $u \times v$ arrays with the structure of a $\mathbb{C}$-vector space. Entries of arrays are usually taken from a finite multiplicative subgroup of $\mathbb{C} \setminus \{0\}$ (and possibly 0), the *alphabet* of the array.

Throughout the paper, for a complex number $z \in \mathbb{C}$ we denote its complex conjugate by z^* and the complex norm by $|z| = \sqrt{zz^*}$.

2.1. Autocorrelation. In the following, let $A, B \in \mathbb{M}_{u,v}(\mathbb{C})$.

The *complex conjugate* $A^* \in \mathbb{M}_{u,v}(\mathbb{C})$ of a $u \times v$ array A has entries $A^*[i, j] = (A[i, j])^*$. The *convolution array* of A and B is the array $A \circledast B \in \mathbb{M}_{u,v}(\mathbb{C})$ with entries

$$(A \circledast B)[k, l] = \sum_{i=0}^{u-1} \sum_{j=0}^{v-1} A[i, j]B[k - i, l - j].$$

It follows that "$\circledast$" is a commutative and associative multiplication of arrays, which furnishes the $\mathbb{C}$-space $\mathbb{M}_{u,v}(\mathbb{C})$ with the structure of a $\mathbb{C}$-algebra, cf. [4].

Definition 2.2. We denote by $\mathcal{A} = \mathcal{A}_{u,v}$ the $\mathbb{C}$-algebra $\mathbb{M}_{u,v}(\mathbb{C})$ with multiplication "$\circledast$" and component-wise addition and scalar multiplication. We denote by $\mathbf{0} = \mathbf{0}_{u,v} \in \mathcal{A}$ the array with only zero entries.

The *cross-correlation array* of A and B is the array $\mathbf{CC}(A, B) \in \mathcal{A}$ with entries

$$\mathbf{CC}(A, B)[k, l] = \sum_{i=0}^{u-1} \sum_{j=0}^{v-1} A[i, j]B^*[i + k, j + l].$$

The *autocorrelation array* of A is $\mathbf{AC}(A) = \mathbf{CC}(A, A)$. The *peak autocorrelation* of A is the entry

$$\mathbf{AC}(A)[0, 0] = \sum_{i=0}^{u-1} \sum_{j=0}^{v-1} |A[i, j]|^2;$$

the other entries of $\mathbf{AC}(A)$ are the *off-peak autocorrelations* of A. If the entries of A are roots of unity, with perhaps a few zeroes, then each $|A[i, j]|^2$ is 0 or 1, and the peak autocorrelation is a nonnegative integer of value at most uv. Clearly, $A = \mathbf{0}$ if and only if $\mathbf{AC}(A) = 0$.

The final publication is available at Springer via
http://dx.doi.org/10.1007/s12095-017-0214-0

As indicated in the introduction, arrays with low off-peak autocorrelation are widely sought in applications. Of particular interest are so-called perfect and almost perfect arrays.

Definition 2.3. Let $A \in \mathcal{A}_{u,v}$ be a $u \times v$ array.

a) The array A is *perfect* if all off-peak autocorrelations are zero.

b) The array A is *almost perfect* if u is even, $\mathbf{AC}(A)[0,0] = uv = -\mathbf{AC}(A)[u/2,0]$, and all other off-peak autocorrelations are zero.

For more information on perfect arrays we refer to [3, 7, 8]. The above definition of "almost perfect" is from [1]; other definitions exist. We generalise this concept as follows.

Definition 2.4. Let $n \geq 2$ be an integer. An array $A \in \mathcal{A}_{u,v}$ is *n-perfect* if u is divisible by n, and the only nonzero off-peak autocorrelations are

$$\mathbf{AC}(A)[iu/n, 0] = uv\lambda^i \quad \text{for} \quad i = 0, \ldots, n-1,$$

where λ is a primitive n-th root of unity.

An n-perfect array thus has an autocorrelation array with the n-th roots of unity in sequence (scaled by the size of the array) equally spaced down the first column, and zeroes everywhere else; see Example 3.2 below. Clearly, the 2-perfect arrays are exactly the almost perfect arrays as defined in [1]. To describe our main result, a recursive construction of n-perfect arrays, we first need to introduce more notation.

2.2. Basic array operations.

We briefly recall some operations on arrays from [4, 5].

Let $A, B \in \mathcal{A} = \mathcal{A}_{u,v}$. The *reversal* $A^r \in \mathcal{A}$ of A is the array with entries $A^r[i,j] = A[-i,-j]$; it follows from the definition that $(A \circledast B)^r = A^r \circledast B^r$. Let $z \in \mathbb{Z}$; the *z-column shift* (or *vertical shear*) $A^{c_z} \in \mathcal{A}$ of A is the array with entries $A^{c_z}[i,j] = A[i + zj, j]$; in other words, A^{c_z} is the array A with the j-th column shifted cyclically zj places up.

The *horizontal concatenation* $H = \mathbf{H}(A_0, \ldots, A_{r-1})$ of arrays $A_0, \ldots, A_{r-1} \in \mathcal{A}$ is the $u \times rv$ array with entries $H[i,j] = A_{\lfloor j/r \rfloor}[i, j \bmod v]$, where $j \bmod v$ is the remainder of the division of j by v and $\lfloor j/r \rfloor$ is the quotient of the division of j by r. The *vertical concatenation* $V = \mathbf{V}(A_0, \ldots, A_{r-1})$ is the $ru \times v$ array with entries $V[i,j] = A_{\lfloor i/r \rfloor}[i \bmod u, j]$. The *row interleaving* $R = \mathbf{R}(A_0, \ldots, A_{r-1})$ is the $ru \times v$ array with entries $R[i,j] = A_{i \bmod r}[\lfloor i/r \rfloor, j]$.

Example 2.5. If

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{bmatrix},$$

then

$$A^r = \begin{bmatrix} 1 & 3 & 2 \\ 7 & 9 & 8 \\ 4 & 6 & 5 \end{bmatrix}, \quad A^{c_1} = \begin{bmatrix} 1 & 5 & 9 \\ 4 & 8 & 3 \\ 7 & 2 & 6 \end{bmatrix}, \quad \mathbf{R}(A,B) = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 4 & 5 & 6 \\ 2 & 2 & 2 \\ 7 & 8 & 9 \\ 3 & 3 & 3 \end{bmatrix}, \quad \mathbf{H}(A,B) = \begin{bmatrix} 1 & 2 & 3 & 1 & 1 & 1 \\ 4 & 5 & 6 & 2 & 2 & 2 \\ 7 & 8 & 9 & 3 & 3 & 3 \end{bmatrix}.$$

3. A recursive construction of n-perfect arrays

Starting with an n-perfect array A of size $nu \times v$ with $v \mid u$, we now construct an n-perfect array of size $n^2u \times nv$, and, iteratively, of size $n^{k+1}u \times n^k v$ for all $k \geq 1$.

Theorem 3.1. *Let $A \in \mathcal{A}_{nu,v}$ be n-perfect with $v \mid u$. Let $B_0 = \mathbf{H}(A, \ldots, A)$ be the horizontal concatenation of n copies of A, and set $B_k = B_0^{c_{ku/v}}$ for $k = 1, \ldots, n-1$. Then the row interleaving $C = \mathbf{R}(B_0, \ldots, B_{n-1})$ is an n-perfect array of size $n^2u \times nv$.*

The proof of Theorem 3.1 is rather technical and will be given in Section 4; we end this section with a series of examples. Theorem 3.4 below provides a variety of n-perfect $n^2 \times n$ arrays which can be used as the seed of the recursive construction in Theorem 3.1, yielding n-perfect arrays of size $n^{k+1} \times n^k$ for all $k \geq 1$.

Example 3.2. We consider $n = 3$ and $u = v = 1$; let $\lambda \in \mathbb{C}$ be a primitive 3rd root of unity. We apply the construction in Theorem 3.1 to the 3-perfect array

$$A = \begin{bmatrix} 1 \\ \lambda^2 \\ \lambda \end{bmatrix} \quad \text{with} \quad \mathbf{AC}(A) = 3 \begin{bmatrix} 1 \\ \lambda \\ \lambda^2 \end{bmatrix}.$$

The horizontal concatenation of 3 copies of A is

$$B_0 = \mathbf{H}(A, A, A) = \begin{bmatrix} 1 & 1 & 1 \\ \lambda^2 & \lambda^2 & \lambda^2 \\ \lambda & \lambda & \lambda \end{bmatrix},$$

and the arrays B_1 and B_2 are

$$B_1 = B_0^{c_1} = \begin{bmatrix} 1 & \lambda^2 & \lambda \\ \lambda^2 & \lambda & 1 \\ \lambda & 1 & \lambda^2 \end{bmatrix} \quad \text{and} \quad B_2 = B_0^{c_2} = \begin{bmatrix} 1 & \lambda & \lambda^2 \\ \lambda^2 & 1 & \lambda \\ \lambda & \lambda^2 & 1 \end{bmatrix}.$$

Interleaving the rows of B_0, B_1, B_2 gives

$$C = \mathbf{R}(B_0, B_1, B_2) = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \lambda^2 & \lambda \\ 1 & \lambda & \lambda^2 \\ \lambda^2 & \lambda^2 & \lambda^2 \\ \lambda^2 & \lambda & 1 \\ \lambda^2 & 1 & \lambda \\ \lambda & \lambda & \lambda \\ \lambda & 1 & \lambda^2 \\ \lambda & \lambda^2 & 1 \end{bmatrix} \quad \text{with} \quad \mathbf{AC}(C) = 27 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \lambda & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ \lambda^2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$

so C is indeed 3-perfect. One can now repeatedly apply Theorem 3.1 to obtain an infinite sequence of 3-perfect arrays of size $3^{k+1} \times 3^k$ with $k \geq 0$.

The construction in Example 3.2 can easily be generalised to construct an n-perfect $n^2 \times n$ array C from an n-perfect $n \times 1$ array A with entries $A[i, 0] = \lambda^{n-i}$, where λ is a primitive n-th root of unity. Moreover, the entries of C can be stated directly, as done in the next theorem; recall that $\lfloor i/n \rfloor$ denotes the quotient of the division with remainder of i by n. To prove the theorem, we require the following well-known result, see for example [9, Ex. 2.1].

Lemma 3.3. *Let λ be a primitive n-th root of unity, $n \geq 2$. If $a \in \mathbb{Z}$ is an integer, then*

$$\sum_{i=0}^{n-1} (\lambda^a)^i = \begin{cases} n & \text{if } n \mid a \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 3.4. *Let $n \geq 2$ be an integer and fix a primitive n-th root of unity $\lambda \in \mathbb{C}$ and coefficients $\alpha, \beta, \gamma \in \mathbb{Z}$ with $\alpha \neq 0$ coprime to n. Then the following hold.*

a) *The $n \times 1$ array A with entries $A[i, 0] = \lambda^{n-i}$ is n-perfect.*

b) *The $n \times n$ array B with entries $B[i, j] = \lambda^{\alpha ij + \beta i + \gamma j}$ is perfect with peak entry n^2.*

c) *The $n^2 \times n$ vertical concatenation $C = \mathbf{V}(\lambda^n B, \lambda^{n-1} B, \ldots, B)$ has entries*

$$C[i, j] = \lambda^{\alpha ij + \beta i + \gamma j - \lfloor i/n \rfloor}$$

and is n-perfect.

Before we prove this theorem we note that the 9×3 array C in Example 3.2 corresponds to the array C in Theorem 3.4 with $n = 3$ and coefficients $\alpha = -1$ and $\beta = \gamma = 0$.

PROOF OF THEOREM 3.4. a) The entries of $\mathbf{AC}(A)$ are

$$\mathbf{AC}(A)[s, 0] = \sum_{i=0}^{n-1} A[i, 0] A^*[s + i, 0] = \sum_{i=0}^{n-1} \lambda^{n-i} \lambda^{-(n-s-i)} = n\lambda^s,$$

which proves that A is n-perfect.

b) The entries of $\mathbf{AC}(B)$ are

$$\begin{aligned} \mathbf{AC}(B)[s, t] &= \sum_{i,j=0}^{n-1} B[i, j] B^*[i + s, j + t] \\ &= \sum_{i,j=0}^{n-1} \lambda^{\alpha ij + \beta i + \gamma j - \alpha(i+s)(j+t) - \beta(i+s) - \gamma(j+t)} \\ &= \lambda^{-\alpha st - \gamma t - \beta s} \sum_{i=0}^{n-1} (\lambda^{-\alpha t})^i \sum_{j=0}^{n-1} (\lambda^{-\alpha s})^j. \end{aligned}$$

Since $\alpha \neq 0$ is coprime to n, Lemma 3.3 shows that B is a perfect array with peak entry n^2.

c) First, if $j \in \{0, \ldots, n-1\}$ and $i = qn + r \in \{0, \ldots, n^2 - 1\}$ with $q \in \mathbb{Z}$ and $r \in \{0, \ldots, n-1\}$, then indeed

$$C[i, j] = \lambda^{n-q} B[r, j] = \lambda^{n-q} \lambda^{\alpha rj + \beta r + \gamma j} = \lambda^{\alpha rj + \beta r + \gamma j - \lfloor i/n \rfloor}.$$

If $s \in \{0, \dots, n^2-1\}$ and $t \in \{0, \dots, n-1\}$, then

$$\begin{aligned}\mathbf{AC}(C)[s,t] &= \sum_{i=0}^{n^2-1} \sum_{j=0}^{n-1} C[i,j]C^*[i+s, j+t] \\ &= \sum_{i=0}^{n^2-1} \sum_{j=0}^{n-1} \lambda^{\alpha ij+\beta i+\gamma j-\lfloor i/n\rfloor-\alpha(i+s)(j+t)-\beta(i+s)-\gamma(j+t)+\lfloor (i+s)/n\rfloor} \\ &= \lambda^{-\alpha st-\gamma t-\beta s} \sum_{i=0}^{n^2-1} (\lambda^{-\alpha t})^i \lambda^{\lfloor (s+i)/n\rfloor-\lfloor i/n\rfloor} \sum_{j=0}^{n-1} (\lambda^{-\alpha s})^j.\end{aligned}$$

As in part b), it follows from Lemma 3.3 that $\mathbf{AC}(C)[s,t] = 0$ if $n \nmid s$, and it remains to consider $\tilde{s} = nx \in \{0, \dots, n^2-1\}$; in this case $\lfloor (s+i)/n\rfloor - \lfloor i/n\rfloor = x$ and we obtain

$$\mathbf{AC}(C)[\tilde{s}, t] = n\lambda^{-\gamma t}\lambda^x \sum_{i=0}^{n^2-1} (\lambda^{-\alpha t})^i.$$

As before, Lemma 3.3 shows that $\mathbf{AC}(C)[\tilde{s}, t] = 0$ whenever $n \nmid t$; if $t = 0$, then we obtain

$$\mathbf{AC}(C)[\tilde{s}, 0] = n^3\lambda^x.$$

In conclusion, if $t \neq 0$ or $n \nmid s$, then $\mathbf{AC}(C)[s,t] = 0$; if $s = xn \in \{0, \dots, n^2-1\}$, then $\mathbf{AC}(C)[xn, 0] = n^3\lambda^x$. Since C has size $n^2 \times n$, this proves that C is n-perfect. □

3.1. Further examples of n-perfect arrays. For integers $n, m \geq 2$ we construct n-perfect arrays of size $n \times m$, usually defined over $\mathrm{lcm}(2m, n)$-th roots of unities.

Theorem 3.5. *Let $n, m \geq 2$ be integers, let $\lambda \in \mathbb{C}$ be a primitive n-th root of unity, and let $A \in \mathcal{A}_{1,m}$ be perfect. The $n \times m$ array C with entries $C[i,j] = \lambda^{-i}A[0,j]$ is n-perfect.*

PROOF. The autocorrelation entries of C are

$$\begin{aligned}\mathbf{AC}(C)[s,t] &= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} C[i,j]C^*[i+s, j+t] \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \lambda^{-i}A[0,j]\lambda^{s+i}A^*[0, j+t] \\ &= n\lambda^s \sum_{j=0}^{m-1} A[0,j]A^*[0,j+t] \\ &= n\lambda^s \mathbf{AC}(A)[0,t].\end{aligned}$$

Now the claim follows from $\mathbf{AC}(A)[0,0] = m$ and $\mathbf{AC}(A)[0,t] = 0$ if $t \neq 0$. □

Our construction in Theorem 3.5 requires a perfect array of size $1 \times m$; examples of such perfect arrays (sequences) are given in [2, Section 3]. In particular, for every m there exists such a sequence, for example, the *Chu sequence* as given in part a) of the following lemma (cf. [2, Section 3.2]); in part b) we list another perfect sequence of prime length.

Lemma 3.6. a) *Let λ be a primitive $2m$-th root of unity, $m > 1$. The $1 \times m$ array A with entries $A[0,j] = \lambda^{e_j}$ is perfect, where $e_j = j^2$ if m is even, and $e_j = j(j+1)$ otherwise.*

b) *Let λ be a primitive p-th root of unity, $p > 2$ a prime. The $1 \times p$ array A with entries $A[0,j] = \lambda^{j(j-1)/2}$ is perfect.*

PROOF. a) See, for example, [2, Section 3.2].

b) We have $A[0,j] = \lambda^{e_j}$ with $e_j = j(j-1)/2$; for simplicity, write $e_j = e_{j \bmod p}$ for $j \in \mathbb{Z}$, and note that $e_j - e_{j+t} = -(tj + t(t-1)/2)$. Since $\mathbb{Z}_p$, the integers modulo p, is a field, each $t \in \{1, \dots, p-1\}$ is a unit in $\mathbb{Z}_p$, and therefore

$$\{-(tj + t(t-1)/2) \bmod p \mid j \in \mathbb{Z}_p\} = \{0, \dots, p-1\}.$$

Thus, if $t \neq 0$, then $\mathbf{AC}(A)[0,t] = \sum_{j=0}^{p-1} \lambda^{e_j - e_{j+t}} = \sum_{j=0}^{p-1} \lambda^j = 0$. Finally, note that $\mathbf{AC}(A)[0,0] = p$, which proves that A is perfect. □

As a corollary, Theorems 3.4 and 3.5 imply that for every $n, m \in \mathbb{N}$ there exists an n-perfect array of size $n \times m$, defined over $\mathrm{lcm}(2m, n)$-th roots of unity. We end this section with an example of a 4-perfect 4×4 array which is defined over 4-th roots of unity.

Example 3.7. Let $\imath$ be a primitive 4-th root of unity; the array

$$C = \begin{bmatrix} 1 & 1 & 1 & -1 \\ -\imath & -\imath & -\imath & \imath \\ -1 & -1 & -1 & 1 \\ \imath & \imath & \imath & -\imath \end{bmatrix} \quad \text{satisfies} \quad \mathbf{AC}(C) = 16 \begin{bmatrix} 1 & 0 & 0 & 0 \\ \imath & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ -\imath & 0 & 0 & 0 \end{bmatrix},$$

and therefore is 4-perfect.

4. Proof of the recursive construction

We now prove Theorem 3.1; for this purpose, we start with a series of preliminary results.

4.1. Preliminary results. Our construction of n-perfect arrays in Theorem 3.1 uses array concatenation, column shifts, and row interleaving. In this section we study how these operations affect the autocorrelation of an array. Unless stated otherwise, let $\mathcal{A} = \mathcal{A}_{u,v}$.

Lemma 4.1. *If $A, B \in \mathcal{A}$, then $\mathbf{AC}(\mathbf{CC}(A, B)) = \mathbf{AC}(A)^r \circledast \mathbf{AC}(B)^r$.*

Lemma 4.1 follows implicitly from the proof of [1, Lem. 25]. A direct and simpler proof, in terms of the algebra $\mathcal{A}$, is given in our paper, see [4, Thm 4.8]: one main ingredient in our proof is the fact that reverse distributes over array convolution, that is, if $A, B \in \mathcal{A}$, then $(A \circledast B)^r = A^r \circledast B^r$.

Lemma 4.2. *Let $A \in \mathcal{A}$ and let $B = \mathbf{H}(A, \ldots, A)$ be the horizontal concatenation of $k \geq 1$ copies of A. Then $\mathbf{AC}(B) = k \cdot \mathbf{H}(\mathbf{AC}(A), \ldots, \mathbf{AC}(A))$ is the horizontal concatenation of k copies of $\mathbf{AC}(A)$ with every entry multiplied by k.*

PROOF. By definition, $B[i, j] = A[i, j] = A[i \bmod u, j \bmod v]$ for all $i \in \{0, \ldots, u-1\}$ and $j \in \{0, \ldots, kv-1\}$, thus

$$\mathbf{AC}(B)[s, t] = \sum_{i=0}^{u-1} \sum_{j=0}^{kv-1} A[i, j]A^*[i+s, j+t].$$

As j goes from 0 to $kv-1$, the value $j \bmod v$ goes from 0 to $v-1$ a total of k times; thus we have

$$\mathbf{AC}(B)[s, t] = k \sum_{i=0}^{u-1} \sum_{j=0}^{v-1} A[i, j]A^*[i+s, j+t] = k\mathbf{AC}(A)[s, t];$$

by definition, $\mathbf{AC}(A)[s, t] = \mathbf{AC}(A)[s \bmod u, t \bmod v]$, which proves the assertion. □

Lemma 4.3. *Let $z \in \mathbb{Z}$ and $A \in \mathcal{A}$; the z-column shift satisfies $\mathbf{AC}(A^{c_z}) = \mathbf{AC}(A)^{c_z}$.*

PROOF. Recall that $A^{c_z}[i, j] = A[i + zj, j]$; the claim now follows from a straightforward calculation which involves a variable substitution $i' = i + zj$:

$$\begin{aligned} \mathbf{AC}(A^{c_z})[s, t] &= \sum_{i=0}^{u-1} \sum_{j=0}^{v-1} A[i + zj, j]A^*[i + s + z(j + t), j + t] \\ &= \sum_{j=0}^{v-1} \sum_{i=0}^{u-1} A[i + zj, j]A^*[(i + zj) + (s + zt), j + t] \\ &= \sum_{j=0}^{v-1} \sum_{i'=0}^{u-1} A[i', j]A^*[i' + (s + zt), j + t] \\ &= \mathbf{AC}(A)[s + zt, t] \\ &= \mathbf{AC}(A)^{c_z}[s, t]. \end{aligned}$$

□

The next lemma requires more notation; for integers $a, b \in \mathbb{Z}$ set

$$\delta_n(a, b) = \begin{cases} 0 & \text{if } (a \bmod n) + (b \bmod n) < n \\ 1 & \text{otherwise,} \end{cases}$$

so that

$$\lfloor (a + b)/n \rfloor = \lfloor a/n \rfloor + \lfloor b/n \rfloor + \delta_n(a, b). \tag{4.1}$$

Lemma 4.4. *Let $A_0, \ldots, A_{r-1} \in \mathcal{A}$ with $r \geq 1$, and denote by $B = \mathbf{R}(A_0, \ldots, A_{r-1})$ their row interleaving. The entries of $\mathbf{AC}(B)$ are*

$$\mathbf{AC}(B)[s, t] = \sum_{y=0}^{r-1} \mathbf{CC}(A_y, A_{(y+s) \bmod r})[\lfloor s/r \rfloor + \delta_r(y, s), t];$$

in particular, if $r \mid s$, then $\mathbf{AC}(B)[s, t] = \sum_{y=0}^{r-1} \mathbf{AC}(A_y)[s/r, t]$.

The final publication is available at Springer via
http://dx.doi.org/10.1007/s12095-017-0214-0

PROOF. To simplify notation, we write $A_i = A_{i \bmod r}$ for $i \in \mathbb{Z}$. By the definition of row interleaving, $B[i,j] = A_i[\lfloor i/r \rfloor, j]$, so the entries of $\mathbf{AC}(B)$ are

$$\begin{aligned}\mathbf{AC}(B)[s,t] &= \sum_{i=0}^{ru-1} \sum_{j=0}^{v-1} A_i[\lfloor i/r \rfloor, j] A^*_{i+s}[\lfloor (i+s)/r \rfloor, j+t] \\ &\overset{(4.1)}{=} \sum_{i=0}^{ru-1} \sum_{j=0}^{v-1} A_i[\lfloor i/r \rfloor, j] A^*_{i+s}[\lfloor i/r \rfloor + \lfloor s/r \rfloor + \delta_r(i,s), j+t].\end{aligned}$$

The map $(x,y) \mapsto (xr+y)$ is a bijection from $\mathbb{Z}_u \times \mathbb{Z}_r$ to $\mathbb{Z}_{ru}$; making the substitution $i = xr + y$ so that $\lfloor i/r \rfloor = x$ and $i \bmod r = y$, the assertion follows from

$$\begin{aligned}\mathbf{AC}(B)[s,t] &= \sum_{y=0}^{r-1} \sum_{x=0}^{u-1} \sum_{j=0}^{v-1} A_y[x,j] A^*_{y+s}[x + \lfloor s/r \rfloor + \delta_r(y,s), j+t] \\ &= \sum_{y=0}^{r-1} \mathbf{CC}(A_y, A_{y+s})[\lfloor s/r \rfloor + \delta_r(y,s), t]. \qquad \square\end{aligned}$$

4.2. The proof. For convenience, we restate the main theorem.

Theorem 3.1. *Let $A \in \mathcal{A}_{nu,v}$ be n-perfect with $v \mid u$. Let $B_0 = \mathbf{H}(A, \dots, A)$ be the horizontal concatenation of n copies of A, and set $B_k = B_0^{c_{ku/v}}$ for $k = 1, \dots, n-1$. Then the row interleaving $C = \mathbf{R}(B_0, \dots, B_{n-1})$ is an n-perfect array of size $n^2 u \times nv$.*

PROOF. Let λ be a primitive n-th root of unity such that

$$\mathbf{AC}(A)[i,j] = \begin{cases} nuv\lambda^{i/u} & \text{if } u \mid i \text{ and } j = 0 \\ 0 & \text{otherwise.} \end{cases}$$

An application of Lemma 4.2 yields

$$\mathbf{AC}(B_0)[i,j] = \begin{cases} n^2uv\lambda^{i/u} & \text{if } u \mid i \text{ and } v \mid j \\ 0 & \text{otherwise.} \end{cases}$$

By Lemma 4.3, we have $\mathbf{AC}(B_k) = \mathbf{AC}(B_0)^{c_{ku/v}}$ for all $k = 0, \dots, n-1$; thus

$$\begin{aligned}\mathbf{AC}(B_k)[i,j] &= \mathbf{AC}(B_0)[i + jku/v, j] \\ &= \begin{cases} n^2uv\lambda^{i/u + jk/v} & \text{if } u \mid i \text{ and } v \mid j \\ 0 & \text{otherwise;} \end{cases} \qquad (4.2)\end{aligned}$$

note that $u \mid (i + juk/v)$ with $v \mid j$ if and only if $u \mid i$.

If $u \mid i$ and $v \mid j$, say $i = ua$ and $j = vb$ with $a, b \in \{0, \dots, n-1\}$, then

$$\sum_{k=0}^{n-1} \mathbf{AC}(B_k)[i,j] = \sum_{k=0}^{n-1} n^2uv\lambda^{a+bk} = n^2uv\lambda^a \sum_{k=0}^{n-1} (\lambda^b)^k,$$

and together with Lemma 3.3, we deduce that

$$\sum_{k=0}^{n-1} \mathbf{AC}(B_k)[i,j] = \begin{cases} n^3uv\lambda^{i/u} & \text{if } u \mid i \text{ and } j = 0 \\ 0 & \text{otherwise.} \end{cases}$$

We now claim that $\mathbf{CC}(B_k, B_l) = \mathbf{0}$ whenever $k \neq l$. To prove this, let $k \neq l$ and note that

$$(\mathbf{AC}(B_k) \circledast \mathbf{AC}(B_l))[s,t] = \sum_{i=0}^{nu-1} \sum_{j=0}^{nv-1} \mathbf{AC}(B_k)[i,j] \mathbf{AC}(B_l)[s-i, t-j].$$

By (4.2), in the right hand sum, each summand with $u \nmid i$, $u \nmid s$, $v \nmid j$, or $v \nmid t$ is zero; thus it remains to consider $s = ua$ and $t = vb$ with $a, b \in \mathbb{Z}$, so that

$$\begin{aligned}(\mathbf{AC}(B_k) \circledast \mathbf{AC}(B_l))[s,t] &= \sum_{i,j=0}^{n-1} \mathbf{AC}(B_k)[iu, jv] \mathbf{AC}(B_l)[au - iu, bv - jv] \\ &= \sum_{i,j=0}^{n-1} n^2uv\lambda^{i+jk} n^2uv\lambda^{a-i+l(b-j)} \\ &= n^4u^2v^2\lambda^{a+bl} \sum_{i,j=0}^{n-1} (\lambda^{(k-l)})^j,\end{aligned}$$

hence $(\mathbf{AC}(B_k) \circledast \mathbf{AC}(B_l))[s,t] = 0$ by Lemma 3.3; recall that $k, l \in \{0, \dots, n-1\}$ with $k \neq l$. In conclusion, $\mathbf{AC}(B_k) \circledast \mathbf{AC}(B_l) = \mathbf{0}$, hence also $\mathbf{AC}(B_k)^r \circledast \mathbf{AC}(B_l)^r = \mathbf{0}$. Now Lemma 4.1 yields $\mathbf{AC}(\mathbf{CC}(B_k, B_l)) = \mathbf{0}$, which implies that $\mathbf{CC}(B_k, B_l) = \mathbf{0}$.

We can now show that C is n-perfect. Recall that C is the row interleaving of $B_0, \ldots, B_{n-1}$; Lemma 4.4 shows that

$$\mathbf{AC}(C)[s,t] = \sum_{y=0}^{n-1} \mathbf{CC}(B_y, B_{(y+s) \bmod n})[\lfloor s/n \rfloor + \delta_n(y,s), t]. \tag{4.3}$$

If $n \nmid s$, then $y \not\equiv (y+s) \bmod n$, hence $\mathbf{CC}(B_y, B_{(y+s) \bmod n}) = \mathbf{0}$ as shown above; in this case, $\mathbf{AC}(C)[s,t] = 0$, and it remains to consider $n \mid s$, say $s = na$. Together with (4.2) and Lemma 4.4, Equation (4.3) reduces to

$$\mathbf{AC}(C)[na,t] = \sum_{y=0}^{n-1} \mathbf{AC}(B_y)[a,t] = \begin{cases} n^3 uv\lambda^{a/u} & \text{if } u \mid a \text{ and } t = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Note that if $n \nmid s$, then $nu \nmid s$, and that $s = an$ coupled with $u \mid a$ implies $nu \mid s$. With these facts in mind, the above two paragraphs imply that the entries of $\mathbf{AC}(C)$ are

$$\mathbf{AC}(C)[s,t] = \begin{cases} n^3 uv\lambda^{s/nu} & \text{if } nu \mid s \text{ and } t = 0 \\ 0 & \text{otherwise,} \end{cases}$$

which proves that C is n-perfect. Clearly, C is defined over the same alphabet as A. □

5. Conclusion

This paper presents a new class of arrays ("n-perfect arrays") with low autocorrelation, extending the classes of perfect arrays ("1-perfect arrays") and almost-perfect arrays ("2-perfect arrays"). Throughout, arrays are considered as elements in a certain matrix algebra. This algebraic set-up has proven to be very useful for describing the autocorrelation of certain array constructions (see Section 4.1) and a recursive construction of n-perfect arrays of increasing size (see Section 4.2). Starting with an n-perfect array of size $nu \times v$ with $v \mid u$, this construction yields n-perfect arrays of size $n^{k+1}u \times n^k v$ for all $k \geq 1$.

References

[1] K. T. Arasu and W. de Launey. *Two-dimensional perfect quaternary arrays*. IEEE Trans. Inform. Theory **47** (2001), no. 4, 1482–1493

[2] S. T. Blake, T. E. Hall, and A. Z. Tirkel. *Arrays over roots of unity with perfect autocorrelation and good ZCZ cross-correlation*. Adv. Math. Commun. **7** (2013), no. 3, 231–242.

[3] L. Bömer and M. Antweiler. *Two-dimensional perfect binary arrays with 64 elements*. IEEE Trans. Inform. Theory **36** (1990), no. 6, 1487-1494.

[4] N. Jolly. *An algebra of arrays and almost perfect watermarks*. Cryptogr. Commun. **7** (2015), no. 4, 363-377.

[5] N. Jolly. *Recursive constructions of arrays with low autocorrelation*. PhD thesis, Monash University, Australia, 2015.

[6] S. Katzenbeisser and F. A. P. Petticolas. Information hiding techniques for steganography and digital watermarking. Artech House, Boston, London. Computer Security Series, 2000.

[7] H. D. Luke. *Sequences and arrays with perfect periodic correlation*. IEEE Trans. Aerosp. Electron. Syst. **24** (1988), 287–294.

[8] H. D. Luke, L. Bömer, and M. Antweiler. *Perfect binary arrays*. Signal Process. **17** (1989) 69–80.

[9] P. J. McCarthy. Introduction to arithmetical functions. Universitext, Springer-Verlag, 1986.

[10] O. Moreno and S. V. Maric. *A new family of frequency–hop codes.* IEEE Trans. Commun. **48** (2000), no. 8, 1241–1244.

[11] O. Moreno, A. Z. Tirkel, U. Parampalli, and R. G. Van Schyndel. *New families of arrays in two dimensions for watermarking applications.* Electronics Letters **46** (2010) no. 22, 1–2.

[12] R. A. Scholtz, P. V. Kumar, and C. J. Corrada-Bravo. *Signal design for ultra-wideband radio, sequences and their applications*. (Sequences and their applications - SETA 2001) May, 2001.

[13] M. R. Schroeder. Number theory in science and communication. 3rd ed., Springer-Verlag, 1997.

[14] E. S. Shivaleela, K. N. Sivarajan, and A. Selvarajan. *Design of a new family of two-dimensional codes for fiber-optic CDMA networks*. J. Lightwave Technol. **16** (1998), no. 4, 501–508.

[15] A. Z. Tirkel, C. F. Osborne, and T. E. Hall. *Steganography–applications of coding theory*. IEEE-IT Workshop, pp. 5759, Svalbord, Norway, 1997.

[16] A. Z. Tirkel, G. A. Rankin, R. M. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne. *Electronic water mark*. DICTA-93 Macquarie University, Sydney (December 1993), 666–672.

[17] R. van Schyndel, A. Z. Tirkel, and I. D. Svalbe. *A multiplicative color watermark*. IEEE-EURASIP Workshop on Non-Linear Signal and Imaging Processing, Antalya, Turkey (1999), 336–340.