Rectangular, Range, and Restricted AONTs: Three Generalizations of All-or-Nothing Transforms

Navid Nasr Esfahani and Douglas R. Stinson*

David R. Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, N2L 3G1
Canada

November 10, 2021

Abstract

All-or-nothing transforms (AONTs) were originally defined by Rivest [14] as bijections from s input blocks to s output blocks such that no information can be obtained about any input block in the absence of any output block. Numerous generalizations and extensions of all-or-nothing transforms have been discussed in recent years, many of which are motivated by diverse applications in cryptography, information security, secure distributed storage, etc. In particular, t-AONTs, in which no information can be obtained about any t input blocks in the absence of any t output blocks, have received considerable study.

In this paper, we study three generalizations of AONTs that are motivated by applications due to Pham et al. [13] and Oliveira et al. [12]. We term these generalizations rectangular, range, and restricted AONTs. Briefly, in a rectangular AONT, the number of outputs is greater than the number of inputs. A range AONT satisfies the t-AONT property for a range of consecutive values of t. Finally, in a restricted AONT, the unknown outputs are assumed to occur within a specified set of "secure" output blocks. We study existence and non-existence and provide examples and constructions for these generalizations. We also demonstrate interesting connections with combinatorial structures such as orthogonal arrays, split orthogonal arrays, MDS codes and difference matrices.

1 Introduction

Rivest [14] defined all-or-nothing transforms in the setting of computational security as a mode of operation for block ciphers that can impede brute-force attacks. Stinson [16] introduced and studied unconditionally secure all-or-nothing transforms, i.e., all-or-nothing transforms in the information-theoretic setting. Various generalizations of these transforms have been studied in recent years, including the following:

- almost AONTs (see [2, 6, 18]),

*D.R. Stinson's research is supported by NSERC discovery grant RGPIN-03882.

- t-AONTS (see [5, 7, 17]), and
- asymmetric AONTS (see [8, 9]).

In this paper, we study three new types of AONTs motivated by applications due to Pham et al. [13] and Oliveira et al. [12]. After introducing each of the generalizations, we study existence and non-existence, and provide examples and constructions.[1] We also demonstrate interesting connections with combinatorial structures such as orthogonal arrays, split orthogonal arrays, MDS codes and difference matrices.

We base all the generalizations in this paper on (t, s, v)-all-or-nothing transforms [2], which are defined informally as follows.

Definition 1.1. *Suppose s is a positive integer and $\phi : \Gamma^s \rightarrow \Gamma^s$, where Γ is a finite set of size v (called an* alphabet*). Thus ϕ is a function that maps an input s-tuple $\mathbf{x} = (x_1, \ldots, x_s)$ to an output s-tuple $\mathbf{y} = (y_1, \ldots, y_s)$. Suppose t is an integer such that $1 \leq t \leq s$.*

*The function ϕ is a (t, s, v)-*all-or-nothing transform *(or a (t, s, v)-AONT) provided that the following properties are satisfied:*

1. *ϕ is a bijection.*
2. *If any $s-t$ of the s outputs $y_1, \ldots, y_s$ are fixed, then the values of any t inputs $x_1, \ldots, x_s$ are completely undetermined.*

It is convenient to define an all-or-nothing transform as a certain combinatorial structure. We recall the relevant combinatorial definitions (e.g., see [5]) and then we briefly review the security provided by these combinatorial structures when they are used as AONTs.

First, we require some preliminary definitions. An (N, k, v)-*array* is an N by k array, say A, whose entries are elements chosen from an alphabet Γ of order v. Suppose the columns of A are labeled by the elements in the set C. Let $D \subseteq C$, and define A_D to be the array obtained from A by deleting all the columns $c \notin D$. We say that A is *unbiased* with respect to D if the rows of A_D contain every $|D|$-tuple of elements of Γ exactly $N/v^{|D|}$ times.

We record the following lemma for future use.

Lemma 1.1. *Suppose that A is an (N, k, v)-array that is unbiased with respect to the set (of columns) D. Then A is unbiased with respect to D' whenever $D' \subseteq D$.*

Here is our combinatorial definition of an AONT.

Definition 1.2. *A (t, s, v)-*all-or-nothing transform *is a $(v^s, 2s, v)$-array, say A, with columns labeled $1, \ldots, 2s$, that is unbiased with respect to the following subsets of columns:*

1. *$\{1, \ldots, s\}$,*
2. *$\{s + 1, \ldots, 2s\}$, and*
3. *$I \cup J$, for all $I \subseteq \{1, \ldots, s\}$ with $|I| = t$ and all $J \subseteq \{s + 1, \ldots, 2s\}$ with $|J| = s - t$.*

We observe that a (t, s, v)-all-or-nothing transform ϕ corresponds to a $(v^s, 2s, v)$-array A in an obvious way. For every input s-tuple $\mathbf{x} = (x_1, \ldots, x_s)$, we create a row of A consisting of the $2s$ entries

$$x_1, \ldots, x_s, y_1, \ldots, y_s,$$

where $(y_1, \ldots, y_s) = \phi(x_1, \ldots, x_s)$. We call A the *array representation* of the AONT ϕ.

[1] These generalizations were first formally defined in the PhD thesis of the first author [4].

Let ϕ be a (t, s, v)-all-or-nothing transform and let A be its array representation. Properties 1 and 2 of Definition 1.2 say that ϕ is a bijection. Property 3 ensures that, if any $s-t$ outputs are fixed, then any t inputs are undetermined.

The security properties of AONTs satisfying Definition 1.2 are investigated in [7] from the standpoint of information theory. We assume an *a priori* distribution on the v^s possible input s-tuples such that every input occurs with positive probability. It is shown in [7] that an AONT satisfying Definition 1.2 has the property that any t inputs take on any possible values with positive probability, given the values of any $s-t$ outputs (this is termed *weak security*). Furthermore, it is proven in [7] that the *a posteriori* information about any t inputs (given the values of any $s-t$ outputs) is equal to the *a priori* information about the t specified inputs if the input s-tuples are equiprobable (this is termed *strong security*).

In the remainder of this paper, we will implicitly be treating AONTs as combinatorial objects that satisfy Definition 1.2.

The following two results are immediate consequences of Definition 1.2.

Theorem 1.2. *[17, Theorem 2.25] A mapping $\phi : \Gamma^s \to \Gamma^s$ is a (t, s, v)-AONT if and only if ϕ^{-1} is an $(s-t, s, v)$-AONT.*

Proof. Interchange the first s and the last s columns of the array representation of ϕ. □

Our second result is an existence result phrased in terms of orthogonal arrays. An *orthogonal array* $\mathrm{OA}(s, k, v)$ is a (v^s, k, v)-array that is unbiased with respect to any subset of s columns.

Theorem 1.3. *[2, Corollary 35] An $OA(s, 2s, v)$ is a (t, s, v)-AONT for all t such that $1 \leq t \leq s$.*

Suppose q is a prime power and the alphabet is $\mathbb{F}_q$. If every output of a (t, s, v)-AONT is an $\mathbb{F}_q$-linear function of the inputs, the AONT is a *linear* (t, s, q)-AONT. We will write a linear (t, s, q)-AONT in the form $\mathbf{y} = \mathbf{x}M^{-1}$, where M is an invertible s by s matrix over $\mathbb{F}_q$ (as always, $\mathbf{x}$ is an input s-tuple and $\mathbf{y}$ is an output s-tuple). Of course this is equivalent to saying that $\mathbf{x} = \mathbf{y}M$.

Theorem 1.4. *[2, Lemma 1] Suppose q is prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Then $\mathbf{y} = \mathbf{x}M^{-1}$ defines a linear (t, s, q)-AONT if and only if all t by t submatrices of M are invertible.*

The next result is an immediate consequence of Theorem 1.2.

Corollary 1.5. *[17, Theorem 2.26] Suppose that $\mathbf{y} = \mathbf{x}M^{-1}$ defines a linear (t, s, q)-AONT. Then $\mathbf{y} = \mathbf{x}M$ defines a linear $(s-t, s, q)$-AONT.*

Now, from Corollary 1.5 and Theorem 1.4, we obtain the following.

Corollary 1.6. *[17] Suppose M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Then $\mathbf{y} = \mathbf{x}M$ defines a linear (t, s, q)-AONT if and only if every $(s-t)$ by $(s-t)$ submatrix of M is invertible.*

In the rest of this section, we will briefly discuss two applications that motivate our three generalizations of AONTs.

Two of the AONT generalizations discussed in this paper are motivated by the work by Oliveira et al. [12], where they considered both the confidentiality and the availability of information distributed and stored on a cloud. More specifically, they studied linear erasure codes that can encode an s-tuple $X \in \mathbb{F}_q^s$ to an $(s+n)$-tuple $Y \in \mathbb{F}_q^{s+n}$, such that any s

symbols from Y can be used to reconstruct X. Furthermore, for a positive integer $t \leq s$, no information can be obtained about any t symbols of X in the absence of any $n+t$ symbols of Y (this is an "AONT-like" property.) This motivates our definition of a *rectangular AONT* that we give in Section 2.

The paper [12] constructed the desired codes using a generator matrix that is an s by $s+n$ super-regular matrix.[2] As indicated in [12], Cauchy matrices can be modified to obtain the desired generator matrices.

One consequence of this Cauchy matrix construction method is that the above-mentioned AONT-like property is satisfied for arbitrary values of t. In fact, Cauchy matrices provide bijections that are simultaneously t-AONTs for all possible relevant values of t, a fact that was noted explicitly in [5, Theorem 6]. This motivates our definition of *range AONTs* (which include the special case of *strong AONTs*) that we give in Section 3.

The second motivating application is due to Pham et al. [13], who studied the use of all-or-nothing transforms in the secure transmission of information across two channels, where one of the channels is using optical encryption to provide security. Their results are valid if the secure channel is achieved using another information theoretically secure scheme, for example, a one-time pad.

In this scenario, the message is broken into input blocks. Output blocks can be computed by applying the transform on the input blocks. Finally, the output blocks are divided into two disjoint subsets, where one of the subsets is of size t. The blocks in the t-subset are sent over the secure channel, while the other blocks are communicated via a public channel. Since we know which output blocks are transmitted over the secure channel, the all-or-nothing transform only needs to satisfy a weaker condition, namely that no information can be obtained about any input block as long as the output blocks that are sent over the secure channel are not available. Consequently, Pham et al. [13] define *restricted AONTs* so that they satisfy this condition. We investigate these AONTs further in Section 4.

2 Rectangular AONTs

We formally define rectangular AONTs as follows.

Definition 2.1. *Suppose s, n, and t are positive integers, where $t \leq s \leq n$. A (t, s, n, v)-*recAONT *is a $(v^s, s+n, v)$ array, with columns labeled $1, \dots, s+n$, that is unbiased with respect to the following sets of columns:*

1. $\{1, \dots, s\}$
2. *any $J \subseteq \{s+1, \dots, s+n\}$ where $|J| = s$*
3. *$I \cup J$, for any sets I and J where $I \subseteq \{1, \dots, s\}$, $|I| = t$, $J \subseteq \{s+1, \dots, s+n\}$ and $|J| = s - t$.*

When $n = s$, we have a (t, s, v)-AONT.

The following result is a straightforward generalization of Theorem 1.3.

Theorem 2.1. *An OA$(s, s+n, v)$, where $n \geq s$, is a (t, s, n, v)-recAONT for all t, $1 \leq t \leq s$.*

[2] A matrix is *super-regular* if all its square submatrices are invertible. The authors of [12] do not require the matrix entries to be nonzero, but we consider the case where all the 1 by 1 submatrices are invertible, i.e., the matrix entries are nonzero.

We now use Theorem 2.1 to give some interesting examples of recAONTs. It is well-known that an OA$(2, k, v)$ is equivalent to a set of $k-2$ mutually orthogonal Latin squares (MOLS) of order v (see, e.g., [15]). Many results on MOLS can be found in the *Handbook of Combinatorial Designs* [1]. These results also provide constructions of recAONTs with $s = 2$ for alphabet sizes that are not required to be a prime power.

For example, suppose we consider $k = 5$. It is well-known that an OA$(2, 5, v)$ exists for all $v \geq 4$, $v \neq 6, 10$ (see [1, p. 126]). Hence, we have the following existence result for recAONT.

Corollary 2.2. *Suppose $v \geq 4$, $v \neq 6, 10$. Then there exists a $(t, 2, 3, v)$-recAONT for $t = 1, 2$.*

We now observe that OA$(2, k, v)$ are equivalent to certain recAONT.

Theorem 2.3. *An OA$(2, k, v)$ is equivalent to a $(1, 2, k-2, v)$-recAONT.*

Proof. Applying Theorem 2.1 with $s = 2$, $t = 1$, it follows that existence of an OA$(2, k, v)$ implies the existence of a $(1, 2, k-2, v)$-recAONT. For the converse, we observe that the array representation of a $(1, 2, k-2, v)$-recAONT is unbiased with respect to any two columns, and hence it is also the array representation of an OA$(2, k, v)$. □

We now discuss a connection between recAONT and split orthogonal arrays, which are structures defined by Levenshtein [10]. A *split orthogonal array* SOA$(t_1, t_2; s_1, s_2; v)$ is a $(v^{t_1+t_2}, s_1 + s_2, v)$-array A that satisfies the following two properties:

1. the columns of A are partitioned into two sets, of sizes s_1 and s_2, and
2. A is unbiased with respect to any set of $t_1 + t_2$ columns, where t_1 columns are chosen from the first set of columns and t_2 columns are chosen from the second set of columns.

The following result due to Bill Martin (private communication) is a straightforward consequence of Definition 2.1.

Theorem 2.4. *Suppose there exists a (t, s, n, v)-recAONT. Then there exists an SOA$(t, s-t; s, n; v)$.*

Proof. From Theorem 2.1 we know that a (t, s, n, v)-recAONT is equivalent to a $(v^s, s+n, v)$-array, that is unbiased with respect to $I \cup J$, for any sets I and J where $I \subseteq \{1, \ldots, s\}$, $|I| = t$, $J \subseteq \{s+1, \ldots, s+n\}$ and $|J| = s-t$. If we set $n_1 = s, n_2 = n, t_1 = t$, and $t_2 = s-t$, then from the definition of split orthogonal arrays, such an array is an SOA$(t, s-t; s, n; v)$. □

Hence, from a design theoretic perspective, rectangular AONTs are structures "between" orthogonal arrays and split orthogonal arrays, in the sense that existence of a suitable orthogonal array implies the existence of a certain recAONT, which in turn implies the existence of a certain split orthogonal array.

Similar to the other types of AONT structures discussed so far, a recAONT is *linear* if its outputs are a linear combination of its inputs. We write a linear recAONT in the form $\mathbf{y} = \mathbf{x}N$, where N is an s by n matrix that satisfies certain properties, as given in the following theorem.

Lemma 2.5. *Suppose that q is a prime power and N is an s by n matrix with entries from $\mathbb{F}_q$. Then $\mathbf{y} = \mathbf{x}N$ defines a linear (t, s, n, q)-recAONT if and only if the following conditions are satisfied:*

1. *every s by s submatrix of N is invertible, and*

2. *every $(s-t)$ by $(s-t)$ submatrix of N is invertible.*

Proof. Clearly property 1 in Definition 2.1 is satisfied if and only if every s by s submatrix of N is invertible. We prove that property 2 holds if and only if every $(s-t)$ by $(s-t)$ submatrix of N is invertible.

Let N' be a matrix consisting of any s columns of N. Then $\mathbf{y}' = \mathbf{x}N'$ is a (t, s, v)-AONT. Therefore, from Corollary 1.6, any $(s-t)$ by $(s-t)$ submatrix of N' is invertible. □

3 Range and Strong AONTs

In this section, we will study *range AONTs*, where the AONT provides the desired security properties for a continuous range of values for t, i.e., for $t_1 \leq t \leq t_2$, for specified integers t_1 and t_2. In particular, if the range consists of all positive integers not exceeding a given integer t, we call the AONT a *strong* AONT. Here is the formal definition, which first appeared in [4].

Definition 3.1. *Suppose s, t_1, and t_2 are positive integers, where $t_1 \leq t_2 \leq s$. A* $([t_1, t_2], s, v)$-rangeAONT *is a $(v^s, 2s, v)$ array, with columns labeled $1, \dots, 2s$, that is unbiased with respect to the following sets of columns:*

1. *$\{1, \dots, s\}$,*
2. *$\{s+1, \dots, 2s\}$,*
3. *$I \cup J$, for any sets I and J where $I \subseteq \{1, \dots, s\}$, $|I| = t$ and $t_1 \leq t \leq t_2$, $J \subseteq \{s+1, \dots, 2s\}$, and $|J| = s - t$.*

Thus, a (t, s, v)-AONT is the exactly the same as a $([t, t], s, v)$-rangeAONT. The following lemma is an immediate consequence of the definition.

Lemma 3.1. *Suppose $t_1 \leq t'_1 \leq t'_2 \leq t_2 \leq s$. Then a $([t_1, t_2], s, v)$-rangeAONT is also a $([t'_1, t'_2], s, v)$-rangeAONT.*

Definition 3.2. *A* (t, s, v)-strong AONT *is a $([1, t], s, v)$-rangeAONT.*

The following corollary is an immediate consequence of Lemma 3.1.

Corollary 3.2. *A* (t, s, v)-strong AONT *is a $([t_1, t_2], s, v)$-rangeAONT if* $1 \leq t_1 \leq t_2 \leq t$.

We should note that (t, s, v)-AONTs are not automatically strong. For example, the optimal linear $(2, p, p)$-AONTs (which exist for all primes p) constructed in [5, 17] are not strong. This is because the relevant matrices M contain 0 entries and hence they are not $(1, p, p)$-AONTs.

The next result follows from Theorem 1.3.

Theorem 3.3. *An $OA(s, 2s, v)$ is an (s, s, v)-strong AONT.*

Similar to the case of t-AONTs, we define a *linear range AONT* as a range AONT such that each output element is a linear function of the input elements. We write a linear range AONT in the form $\mathbf{y} = \mathbf{x}M^{-1}$, where M is an s by s invertible matrix.

Theorem 3.4. *Suppose that q is a prime power and M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Then $\mathbf{y} = \mathbf{x}M^{-1}$ is a $([t_1, t_2], s, q)$-rangeAONT if and only if all t by t submatrices of M are invertible, for all t such that $t_1 \leq t \leq t_2$.*

We give some small examples of linear $(2, p, p)$-strong AONTs. The defining matrices are invertible, they have no 0 entries, and all 2 by 2 submatrices are invertible.

Example 3.1. *A linear* $(2, 2, 3)$*-strong AONT:*

$$\begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Example 3.2. *A linear* $(2, 3, 5)$*-strong AONT:*

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

Example 3.3. *A linear* $(2, 5, 7)$*-strong AONT:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 6 & 2 \\ 1 & 5 & 6 & 2 & 4 \end{pmatrix}.$$

Example 3.4. *A linear* $(2, 6, 9)$*-strong AONT, where* $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$*:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & x & x+1 & x+2 & 2x \\ 1 & x & 2 & 2x & 2x+1 & x+1 \\ 1 & x+1 & 2x+2 & x+2 & 2x & 2x+1 \\ 1 & x+2 & 2x & x & 2x+2 & 2 \\ 1 & 2x & x+2 & 2 & x+1 & x \end{pmatrix}.$$

An s by s Cauchy matrix over $\mathbb{F}_q$ exists if $q \geq 2s$. These matrices are constructed as follows. Let $r_1, \ldots, r_s$, $c_1, \ldots, c_s$ be $2s$ distinct elements of $\mathbb{F}_q$. Then the matrix $M = (m_{ij})$ defined by $m_{ij} = 1/(r_i - c_j)$ is a Cauchy matrix. All square submatrices of an $s \times s$ Cauchy matrix are invertible. Hence, any $s \times s$ Cauchy matrix over $\mathbb{F}_q$ is an (s, s, q)-strong AONT.

For fixed positive integers t_1, t_2 with $t_1 \leq t_2$, and any for prime power q, define

$$\mathcal{S}_R([t_1, t_2], q) = \{s : \text{there exists a linear } ([t_1, t_2], s, q)\text{-rangeAONT}\}.$$

Lemma 3.5. *Suppose that* $q \geq 2t_2$*. Then* $\lfloor \frac{q}{2} \rfloor \in \mathcal{S}_R([t_1, t_2], q)$

Proof. Cauchy matrices yield linear $([t_1, t_2], \lfloor \frac{q}{2} \rfloor, q)$-rangeAONTs, for all t_1 and t_2 such that $1 \leq t_1 \leq t_2 \leq \lfloor \frac{q}{2} \rfloor$. □

Lemma 3.6. *If* $s \in \mathcal{S}_R([t_1, t_2], q)$ *and* $s > t_2$*, then* $s - 1 \in \mathcal{S}_R([t_1, t_2], q)$*.*

Proof. The proof is identical to [5, Theorem 20]. □

Lemma 3.7. *If* $s \in \mathcal{S}_R([t_1, t_2], q)$ *then* $s \leq \max\{q + t_1 - 1, t_1 + 1\}$*.*

Proof. Suppose $s \in \mathcal{S}_R([t_1, t_2], q)$. Then there exists a (t_1, s, q)-AONT. From [5, Theorem 23], there exists an OA(t_1, s, v). Now apply the Bush bound for orthogonal arrays (e.g., see [5, Theorem 24]). □

Suppose $q \geq 2t_2$. In view of Lemmas 3.5–3.7, each set $\mathcal{S}_R([t_1, t_2], q)$ is nonempty and contains a maximum element, which we denote by $M_R([t_1, t_2], q)$. Moreover, $\mathcal{S}_R([t_1, t_2], q)$ contains all positive integers s such that $t_2 \leq s \leq M_R([t_1, t_2], q)$.

The papers [5] and [17] have studied $M_R([2, 2], q)$. We now record some results on $M_R([1, 2], q)$ that can be inferred from results in these papers. Note that $M_R([1, 2], q)$ is simply the largest value of s such that a linear $(2, s, q)$-strong AONT exists.

Theorem 3.8. *For any prime power $q > 2$, $M_R([1, 2], q) \leq q - 1$.*

Proof. Suppose $q > 2$ is prime power. It is shown in [5, Theorem 14] that $M_R([2, 2], q) \leq q$, so it immediately follows that $M_R([1, 2], q) \leq q$. Further, in any $(2, q, q)$-AONT, say $\mathbf{y} = \mathbf{x}M^{-1}$, M contains 0 entries, so the AONT cannot be a 1-AONT (see [5, Lemma 14]). Hence, $M_R([1, 2], q) \leq q - 1$. □

We now observe that the upper bound of Theorem 3.8 can be met whenever $q - 1$ is a Mersenne prime.

Theorem 3.9. *Suppose $2^n - 1$ is a prime. Then $M_R([1, 2], 2^n) = 2^n - 1$.*

Proof. In [5, Theorem 11], it is shown that the transformation $\mathbf{y} = \mathbf{x}M^{-1}$ is a $(2, 2^n - 1, 2^n)$-AONT if M is a Vandermonde matrix defined over $\mathbb{F}_{2^n}$ and $2^n - 1$ is prime. Since a Vandermonde matrix does not contain 0 entries, this transformation is also a $(1, 2^n - 1, 2^n)$-AONT. Hence $M_R([1, 2], 2^n) \geq 2^n - 1$. We also have $M_R([1, 2], 2^n) \leq 2^n - 1$ from Theorem 3.8. □

We have the following improvement of Theorem 3.8 when $q > 3$ is odd.

Theorem 3.10. *For any odd prime power $q > 3$, $M_R([1, 2], q) \leq q - 2$.*

Proof. Suppose $q > 3$ is an odd prime power. In view of Theorem 3.8, we only need to show that a linear $(2, q - 1, q)$-strong AONT does not exist. Suppose that $\mathbf{y} = \mathbf{x}M^{-1}$ is a $(2, q - 1, q)$-strong AONT, where M is a $q - 1$ by $q - 1$ matrix over $\mathbb{F}_q$. We can assume that the first row of M consists of 1 entries. Consider the second and third rows of M (M has at least three rows because $q > 3$). Denote the entries in these rows, from left to right, by $a_1, a_2, \ldots, a_{q-1}$ and $b_1, b_2, \ldots, b_{q-1}$, resp. The a_i's comprise all the nonzero elements of $\mathbb{F}_q$, as do the b_i's.

Now, because q is odd, the product of the a_i's is -1 and the product of the b_i's is also -1. For $1 \leq i \leq q - 1$, define $c_i = a_i / b_i$. Then the product of the c_i's is 1. If the c_i's were all distinct, their product would be $-1 \neq 1$. Therefore there exist distinct indices i and j such that $c_i = c_j$. Hence $a_i b_j = a_j b_i$ and the corresponding 2 by 2 submatrix

$$\begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix}$$

of M is not invertible. This is a contradiction. □

Theorem 3.11. *$M_R([1, 2], 3) = 2$, $M_R([1, 2], 5) = 3$, $M_R([1, 2], 7) = 5$ and $6 \leq M_R([1, 2], 9) \leq 7$.*

Proof. The lower bounds follow from Examples 3.1–3.4. The upper bounds follow from Theorem 3.8 (for $q = 3$) and Theorem 3.10 (for $q > 3$). □

Some of the above results can be interpreted in terms of difference matrices. Let G be an abelian group of order g, written additively, let $2 \leq k \leq g$ and let $\lambda \geq 1$. Then a $(g, k; \lambda)$-*difference matrix* is a k by $g\lambda$ matrix $D = (d_{i,j})$ of entries from G such that, for any two distinct rows i and j of D, the multiset

$$\{d_{i,k} - d_{j,k} : 1 \leq k \leq g\}$$

contains every element of G exactly λ times.

Theorem 3.12. *Suppose q is a prime power. If a $(2, q-1, q)$-strong AONT exists, then a $(q-1, q-1; 1)$-difference matrix with entries from $\mathbb{Z}_{q-1}$ exists.*

Proof. Suppose that $\mathbf{y} = \mathbf{x}M^{-1}$ is a $(2, q-1, q)$-strong AONT, where $M = (m_{i,j})$ is a $q-1$ by $q-1$ matrix over $\mathbb{F}_q$. M contains no 0 entries and all of its 2 by 2 submatrices are invertible. Fix a primitive element $\alpha \in (\mathbb{F}_q)^*$. Every entry $m_{i,j}$ of M can be written uniquely as $m_{i,j} = \alpha^{d_{i,j}}$, where $d_{i,j} \in \mathbb{Z}_{q-1}$. Define $D = (d_{i,j})$. We claim that D is a $(q-1, q-1; 1)$-difference matrix with entries from $\mathbb{Z}_{q-1}$.

Clearly D has entries from $\mathbb{Z}_{q-1}$. Suppose that D is not a difference matrix. Then there are two distinct rows i and j such that

$$d_{i,k} - d_{j,k} = d_{i,\ell} - d_{j,\ell}$$

for some $k \neq \ell$. Then

$$\frac{m_{i,k}}{m_{j,k}} = \frac{m_{i,\ell}}{m_{j,\ell}},$$

so the submatrix

$$\begin{pmatrix} m_{i,k} & m_{i,\ell} \\ m_{j,k} & m_{j,\ell} \end{pmatrix}$$

of M is not invertible. This is a contradiction. □

We can also prove a partial converse to Theorem 3.12.

Theorem 3.13. *Suppose q is a prime power and suppose a $(q-1, q-1; 1)$-difference matrix with entries from $\mathbb{Z}_{q-1}$ exists. Then there is a $q-1$ by $q-1$ matrix M with entries from $\mathbb{F}_q$, such that all 1 by 1 and all 2 by 2 submatrices are invertible.*

Proof. Suppose say $D = (d_{i,j})$ is a $(q-1, q-1; 1)$-difference matrix with entries from $\mathbb{Z}_{q-1}$. Let $\alpha \in (\mathbb{F}_q)^*$ be a primitive element and define $M = (m_{i,j})$ by the rule $m_{i,j} = \alpha^{d_{i,j}}$. M is a $q-1$ by $q-1$ matrix over $\mathbb{F}_q$. Clearly M contains no 0 entries, so all 1 by 1 submatrices are invertible. Suppose a submatrix

$$\begin{pmatrix} m_{i,k} & m_{i,\ell} \\ m_{j,k} & m_{j,\ell} \end{pmatrix}$$

is not invertible. Then we have

$$\begin{aligned} m_{i,k}m_{j,\ell} &= m_{i,\ell}m_{j,k}, \\ d_{i,k} + d_{j,\ell} &= d_{i,\ell} + d_{j,k}, \text{and} \\ d_{i,k} - d_{j,k} &= d_{i,\ell} - d_{j,\ell}, \end{aligned}$$

so D is not a $(q-1, q-1; 1)$-difference matrix. This is a contradiction. □

Remark 3.1. In Theorem 3.13, the matrix M would not yield an AONT unless it is invertible.

Remark 3.2. In view of Theorem 3.12, Theorem 3.10 can also be derived as a special case of [3, Theorem 1.10], which states that a $(g, 3; 1)$-difference matrix over $\mathbb{Z}_g$ does not exist if g is even.

Remark 3.3. The existence or nonexistence of $(2, q-1, q)$-strong AONT is unknown when $q = 2^n$ and $q - 1$ is not prime. Unfortunately, there are no currently known results on difference matrices that can help resolve these cases, either positively or negatively. It has been conjectured (e.g., see [1, Conjecture 5.18, §V.5.3]) that there is no $(g, g\lambda; \lambda)$-difference matrix over any group whose order is not a prime power, but this conjecture has not been proven. If it were proven, then the nonexistence of the above-mentioned AONTS would follow as a consequence of Theorem 3.12.

Remark 3.4. Suppose $2^n - 1$ is prime. We can give an alternate proof of Theorem 3.9 by starting with a particular $(2^n - 1, 2^n - 1; 1)$-difference matrix, namely the multiplication table of $\mathbb{Z}_{2^n-1}$, and applying Theorem 3.12. The resulting matrix M, being a Vandermonde matrix, is invertible, so it yields an AONT.

4 Restricted AONTs

Pham et al. [13] introduced R-restricted AONTs. Their definition, restated in the language of unbiased arrays, is as follows:

Definition 4.1. *Suppose s is a positive integer and $R \subseteq \{1, 2, \cdots, s\}$. An R-restricted AONT is a $(v^s, 2s, v)$ array that is unbiased with respect to the following sets of columns:*

1. $\{1, \ldots, s\}$,
2. $\{s+1, \ldots, 2s\}$,
3. $\{i\} \cup J$, *for any sets* $\{i\}$ *and* J *where* $i \in \{1, \ldots, s\}$, *and* $J = \{s+1, \ldots, 2s\} \setminus R'$, *where* $R' = \{r + s : r \in R\}$. *(Note that we add s to each element of R to obtain R', because R' refers to labels of columns corresponding to outputs of the AONT.)*

Pham et al. [13] use these R-restricted AONTs in a setting where there is an unconditionally secure communication channel, with a limited bandwidth, as well as a channel that can be observed by the adversary. In this setting, a portion of the message is sent through the secure channel, while the rest is transmitted over the regular one. Pham et al. [13] design the security of their system based on the adversary's lack of access to the portion of the message sent over the secure channel. They wish to guarantee that it is impossible for the adversary to gain any information about any one input block, in the absence of the blocks sent over the secure channel. That is, if the output blocks are all known except for the blocks in R', then no information can be obtained about any specific input block.

The above definition can be generalized and extended in various ways. One possible generalization considers the security of any t input blocks, where $t \leq |R|$, in the absence of all the output blocks sent over the secure channel. Our generalization is stronger; we consider the security of any $t \leq |R|$ input blocks assuming that the adversary can learn all the output blocks except for t of the blocks sent over the secure channel. (Of course, if there are exactly t blocks sent over the secure channel, then the adversary is assumed to have access to none of them, and in this case the two generalizations are equivalent.)

Thus, we propose the following more general definition of an R-restricted (t, s, v)-AONT. This definition was first given in [4].

Definition 4.2. *Suppose s is a positive integer, $R \subseteq \{1, 2, \ldots, s\}$, and t is an integer such that $1 \leq t \leq |R|$. An* R-restricted (t, s, v)-AONT *is a $(v^s, 2s, v)$ array with columns, labeled $1, \ldots, 2s$, that is unbiased with respect to the following sets of columns:*

1. $\{1, \ldots, s\}$,
2. $\{s+1, \ldots, 2s\}$,
3. *$I \cup J$, for any sets I and J where $I \subseteq \{1, \ldots, s\}$, $|I| = t$, $J \subseteq \{s+1, \ldots, 2s\}$, $|J| = s-t$, and $|R' \setminus J| = t$, where $R' = \{r + s : r \in R\}$.*

In other words, in an R-restricted (t, s, v)-AONT, fixing all the outputs—except for t outputs in R—does not yield any information about any t inputs.

The following result is an immediate generalization of Theorem 1.3.

Theorem 4.1. *Suppose there exists an $OA(s, 2s, v)$. Let $R \subseteq \{1, 2, \cdots, s\}$. Then there exists an R-restricted (t, s, v)-AONT for all t, $1 \leq t \leq |R|$.*

Suppose $R = \{1, 2, \ldots, \ell\}$, where $\ell \geq t$. The following corollary describes the restricted AONT property in the matrix representation of *linear* restricted AONTs.

Corollary 4.2. *Suppose that q is a prime power, $t \leq \ell$, and M is an invertible s by s matrix with entries from $\mathbb{F}_q$. Then the transformation $\mathbf{y} = \mathbf{x}M^{-1}$ is a $\{1, 2, \ldots, \ell\}$-restricted (t, s, q)-AONT if and only if all t by t submatrices of M that are contained in the first ℓ rows of M are invertible.*

This relaxation of conditions allows for restricted AONTs with parameters for which an AONT does not exist. For instance, it was shown in [5] that $(2, 6, 5)$-AONT and $(2, 9, 9)$-AONT do not exist. However, Examples 4.1 and 4.2 present $\{1, 2\}$-restricted AONTs for the same values of s and q.

Example 4.1. *A linear $\{1, 2\}$-restricted $(2, 6, 5)$-AONT:*

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

Example 4.2. *A linear $\{1, 2\}$-restricted $(2, 9, 9)$-AONT:*

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

When $\ell = t$, Theorem 4.2 requires that any t columns of the t by s submatrix formed by the first t rows of M are linearly independent. To construct such a matrix, we can use the parity check matrix of a maximum distance separable (MDS) code. For example, triply extended Reed-Solomon codes can be used to construct $\{1,2,3\}$-restricted $(3, 2^n+2, 2^n)$-AONTs, as shown in Theorem 4.3.

Theorem 4.3. *Let n be a positive integer and let $q = 2^n$. Then a $\{1,2,3\}$-restricted $(3, 2^n+2, 2^n)$-AONT exists.*

Proof. Let $\omega_1, \omega_2, \ldots, \omega_{q-1}$ be distinct elements in the finite field $\mathbb{F}_q$. The following matrix

$$H = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 & 0 & 0 \\ \omega_1 & \omega_2 & \cdots & \omega_{q-1} & 0 & 1 & 0 \\ {\omega_1}^2 & {\omega_2}^2 & \cdots & {\omega_{q-1}}^2 & 0 & 0 & 1 \end{pmatrix}$$

is the parity check matrix of a triply extended Reed-Solomon code over $\mathbb{F}_q$ (see [11, Ch. 11, Theorem 10]). This code has length $q+2$, dimension $q-1$ and minimum distance 4, so any three columns of H are linearly independent. To construct the AONT, we only need to add $q-1$ additional rows in such a way that the resulting matrix is invertible. This goal can be achieved by choosing rows consisting of a single 1 entry in column i (for $1 \leq i \leq q-2$) and 0's elsewhere. The resulting matrix M gives rise to a $\{1,2,3\}$-restricted $(3, q+2, q)$-AONT. □

Remark 4.1. If we use the dual code of the code used in Theorem 4.3, we can also construct a $\{1, 2, \ldots, q-1\}$-restricted $(q-1, q+2, q)$-AONT.

Doubly extended Reed-Solomon codes can be utilized in the construction of $\{1, 2, \ldots, t\}$-restricted $(t, q+1, q)$-AONTs, as Theorem 4.4 states.

Theorem 4.4. *Let q be a prime power and let $t \leq q+1$. Then a $\{1, 2, \ldots, t\}$-restricted $(t, q+1, q)$-AONT exists.*

Proof. For any value of k such that $1 \leq k \leq q+1$, we can construct a doubly extended Reed-Solomon code of length $q+1$, dimension k and distance $q-k+2$ (see [11, Ch. 11, Theorem 9]). The parity check matrix of this code can be extended by k rows such that the final matrix is invertible. Since any $q-k+1$ columns of the parity check matrix are linearly independent, the final matrix is a $\{1, 2, \ldots, t\}$-restricted $(t, q+1, q)$-AONT, where $t = q-k+1$. □

Remark 4.2. Example 4.1 is an application of Theorem 4.4.

5 Conclusion

In this paper, we have initiated a study of three generalizations and extensions of (t, s, v)-all-or-nothing transforms: rectangular, range, and restricted AONTs. It is worth noting that these properties are not necessarily mutually exclusive. An example of this is the combination of strong and rectangular AONTs that are used in the applications described by Oliveira et al. [12]. Constructions for most of combinations of these AONT properties have not been studied yet and could result in interesting outcomes both in theory and in application.

References

[1] C.J. Colbourn and J.H. Dinitz, eds. *The CRC Handbook of Combinatorial Designs, Second Edition*, CRC Press, 2006.

[2] P. D'Arco, N. Nasr Esfahani and D.R. Stinson. All or nothing at all. *Electronic Journal of Combinatorics* **23(4)** (2016), paper #P4.10, 24 pp.

[3] D.A. Drake. Partial λ-geometries and generalized Hadamard matrices over groups. *Canadian Journal of Mathematics* **31** (1979), 617–727.

[4] N. Nasr Esfahani. *Generalizations of All-or-nothing Transforms and Their Application in Secure Distributed Storage.* PhD thesis, University of Waterloo, 2021.

[5] N. Nasr Esfahani, I. Goldberg and D.R. Stinson. Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets. *IEEE Transactions on Information Theory* **64** (2018), 3136–3143.

[6] N. Nasr Esfahani and D. R. Stinson. Computational results on invertible matrices with the maximum number of invertible 2×2 submatrices. *Australasian Journal of Combinatorics* **69** (2017), 130–144.

[7] N. Nasr Esfahani and D.R. Stinson. On security properties of all-or-nothing transforms. *Designs, Codes and Cryptography* **91** (2021), 2857–2867.

[8] N. Nasr Esfahani and D. R. Stinson. Asymmetric all-or-nothing transforms. To appear in *Mathematical Cryptology.*

[9] G.O. Karame, C. Soriente, K. Lichota and S. Capkun. Securing cloud data under key exposure. *IEEE Transactions on Cloud Computing* **7** (2019), 838–849.

[10] V.I. Levenshtein. Split orthogonal arrays and maximum independent resilient systems of functions. *Designs, Codes and Cryptography* **12** (1997), 131–160.

[11] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1977.

[12] P.F. Oliveira, L. Lima, T. TV Vinhoza, J. Barros, and Mu. Médard. Coding for trusted storage in untrusted networks. *IEEE Transactions on Information Forensics and Security* **7** (2012), 1890–1899.

[13] H. Pham, R. Steinwandt, and A. Suárez Corona. Integrating classical preprocessing into an optical encryption scheme. *Entropy* **21** (2019), 872.

[14] R.L. Rivest. All-or-nothing encryption and the package transform. *Lecture Notes in Computer Science* **1267** (1997), 210–218 (Fast Software Encryption 1997).

[15] D.R. Stinson. *Combinatorial Designs: Constructions and Analysis.* Springer-Verlag, New York, 2004.

[16] D.R. Stinson. Something about all or nothing (transforms). *Designs, Codes and Cryptography* **22** (2001), 133–138.

[17] X. Wang, J. Cui and L. Ji. Linear $(2, p, p)$-AONTs exist for all primes p. *Designs, Codes and Cryptography* **87** (2019), 2185–2197.

[18] Y. Zhang, T. Zhang, X. Wang and G. Ge. Invertible binary matrices with maximum number of 2-by-2 invertible submatrices, *Discrete Mathematics* **340** (2017) 201–208.