entropy

MDPI

Article

Matroidal Entropy Functions: A Quartet of Theories of Information, Matroid, Design, and Coding

Qi Chen [1,*], Minquan Cheng [2,*] and Baoming Bai [1,*]

[1] State Key Laboratory of Integrated Service Networks, Xidian University, Xi' an 710071, China
[2] Guangxi Key Lab of Multi-Source Information Mining & Security, Guangxi Normal University, Guilin 541004, China
* Correspondence: qichen@xidian.edu.cn (Q.C.); chengqinshi@hotmail.com (M.C.); bmbai@mail.xidian.edu.cn (B.B.)

Abstract: In this paper, we study the entropy functions on extreme rays of the polymatroidal region which contain a matroid, i.e., matroidal entropy functions. We introduce variable strength orthogonal arrays indexed by a connected matroid M and positive integer v which can be regarded as expanding the classic combinatorial structure orthogonal arrays. It is interesting that they are equivalent to the partition-representations of the matroid M with degree v and the (M, v) almost affine codes. Thus, a synergy among four fields, i.e., information theory, matroid theory, combinatorial design, and coding theory is developed, which may lead to potential applications in information problems such as network coding and secret-sharing. Leveraging the construction of variable strength orthogonal arrays, we characterize all matroidal entropy functions of order $n \leq 5$ with the exception of $\log 10 \cdot U_{2,5}$ and $\log v \cdot U_{3,5}$ for some v.

Keywords: entropy function; matroidal entropy function; matroid; orthogonal array; variable strength orthogonal array; almost affine code; MDS code; polymatroid

Citation: Chen, Q.; Cheng, M.; Bai, B. Matroidal Entropy Functions: A Quartet of Theories of Information, Matroid, Design, and Coding. *Entropy* **2021**, *23*, 323. https://doi.org/10.3390/e23030323

Academic Editor: Boris Ryabko

Received: 29 December 2020
Accepted: 26 February 2021
Published: 9 March 2021

1. Introduction

Given $N := \{1, 2, \cdots, n\}$ and discrete random vector $\mathbf{X} := (X_i : i \in N)$, the set function $\mathbf{h_X} : 2^N \to \mathbb{R}$ defined by

$$\mathbf{h_X}(A) = H(X_A), \quad \forall A \subseteq N$$

is called the entropy function of $\mathbf{X}$, where $X_A := (X_i : i \in A)$ and $H(X_\emptyset) = 0$ by convention. We also say $\mathbf{X}$ characterizes $\mathbf{h_X}$, or $\mathbf{X}$ is the characterizing random vector of $\mathbf{h_X}$. An entropy function $\mathbf{h}$ can be considered as a vector in the entropy space $\mathcal{H}_n := \mathbb{R}^{2^N}$. (For a set A and a finite set B, A^B denotes the $|B|$ Cartesian product of A with each coordinate indexed by $b \in B$. When $A = \mathbb{F}$ is a field, $\mathbb{F}^B$ is a $|B|$-dimensional vector space over $\mathbb{F}$ with each coordinate indexed by $b \in B$.) We say $\mathcal{H}_n$ and the vectors in it have order n. The set of all entropy functions of order n, denoted by Γ_n^*, is called the entropy region of order n. The closure of Γ_n^*, denoted by $\overline{\Gamma_n^*}$, is called almost entropic region. It is a convex cone [1]. A vector $\mathbf{h} \in \mathcal{H}_n$ is called entropic if $\mathbf{h} \in \Gamma_n^*$, almost entropic if $\mathbf{h} \in \overline{\Gamma_n^*}$, and non-entropic if $\mathbf{h} \notin \Gamma_n^*$. Characterization of entropy functions, i.e., for a vector $\mathbf{h} \in \mathcal{H}_n$, determining whether it is in Γ_n^* or $\overline{\Gamma_n^*}$, is of fundamental importance in information theory.

For a vector $\mathbf{h} \in \mathcal{H}_n$, if it is nonnegative, i.e., $\mathbf{h}(A) \geq 0$ for all $A \subseteq N$, monotone, i.e., $\mathbf{h}(A) \leq \mathbf{h}(B)$ for all $A \subseteq B \subseteq N$, and submodular, i.e., $\mathbf{h}(A \cap B) + \mathbf{h}(A \cup B) \leq \mathbf{h}(A) + \mathbf{h}(B)$ for all $A, B \subseteq N$, the pair $(N, \mathbf{h})$ is called a polymatroid, where N is the ground set and $\mathbf{h}$ is the rank function of the polymatroid. For a polymatroid $(N, \mathbf{h})$, if $\mathbf{h}(A) \in \mathbb{Z}$ and $\mathbf{h}(A) \leq |A|$ for all $A \subset N$, $(N, \mathbf{h})$ is called a matroid. By frequent abuse of terminology, we do not distinguish a (poly)matroid and its rank function if there is no ambiguity. See Section 2.1 for a more detailed discussion on matroids.

The set of all polymatroids in $\mathcal{H}_n$, denoted by Γ_n, is called the polymatroidal region of order n. It is proved in [2] that any entropy function is a polymatroid, thus Γ_n is an outer bound of Γ_n^*. As Γ_n is closed, it is also an outer bound of $\overline{\Gamma_n^*}$. As inequalities bounding Γ_n are equivalent to the nonnegativity of Shannon information measures, they are called Shannon-type information inequalities, and Γ_n is also called the Shannon outer bound of Γ_n^* and $\overline{\Gamma_n^*}$. For more about entropy functions and information inequalities, readers are referred to [3], (Chapter 13–15) [4,5].

It is well known that $\overline{\Gamma_n^*} \subsetneq \Gamma_n$ when $n \geq 4$ due to the existence of non-Shannon-type inequalities, e.g., Zhang-Yeung inequality [6]. However, though $\overline{\Gamma_3^*} = \Gamma_3$, Zhang and Yeung also discovered that on an extreme ray of Γ_3, only countably many vectors are entropic, which implies that $\Gamma_3^* \subsetneq \overline{\Gamma_3^*}$, and therefore there exists a gap between Γ_n^* and $\overline{\Gamma_n^*}$ [1]. Given a random vector $\mathbf{X} = (X_1, X_2, X_3)$ with $X_i, i = 1, 2, 3$ mutually independent and each of them the function of the other two, it is proved in [1] that X_i must be uniformly distributed on a finite set, say $\mathbb{Z}_v := \{0, 1, \cdots, v-1\}$, thus $\mathbf{h}_{\mathbf{X}}(A) = \log v \cdot \min\{2, |A|\}, A \subseteq \{1, 2, 3\}$. On the other hand, for each integer $v \geq 1$, they proved that polymatroid $\mathbf{h}$ with $\mathbf{h}(A) = \log v \cdot \min\{2, |A|\}, A \subseteq \{1, 2, 3\}$ is entropic: let X_1 and X_2 uniformly distributed on $\mathbb{Z}_v$ and $X_3 \equiv X_1 + X_2 \pmod{v}$, then $\mathbf{h}$ is the entropy function of (X_1, X_2, X_3).

As the rank function of $U_{2,3}$ is equal to $\min\{2, |A|\}, A \subseteq \{1, 2, 3\}$, Zhang-Yeung indeed proved that for any vector $\mathbf{h} = c \cdot U_{2,3}$ on the ray $R_{U_{2,3}} := \{c \cdot U_{2,3} : c \geq 0\}$, $\mathbf{h}$ is entropic if and only if $c = \log v$ for some positive integer v. In [7], Matúš proved that, for any extreme ray $R_M := \{c \cdot M : c \geq 0\}$ of Γ_n containing a connected matroid M with rank ≥ 2, $\mathbf{h} = c \cdot M$ is entropic only if $c = \log v$ for some positive integer v. However, on the other hand, $\mathbf{h} = c \cdot M$ is not entropic for all positive integers. For example, we will see in Section 4 that $\mathbf{h} = \log v \cdot U_{2,4}$ is non-entropic when $v = 2, 6$.

Definition 1. *For a connected matroid M with rank ≥ 2, we call the set χ_M of all positive integers v such that $\mathbf{h} = \log v \cdot M$ is entropic the* probabilistically (p-)characteristic *set of M.*

The term p-characteristic set of a matroid M is first coined in [7]. As discussed above, $\chi_{U_{2,3}} = \mathbb{Z}^+$, the set of all positive integers, and $\chi_{U_{2,4}} = \{v \in \mathbb{Z}^+ : v \neq 2, 6\}$. In this paper, we study the p-characteristic set of an arbitrary connected matroid with rank ≥ 2.

Definition 2. *For a connected matroid M with rank ≥ 2 and a positive integer v, if $v \in \chi_M$, we call the entropy function $\mathbf{h} = \log v \cdot M$ a* matroidal entropy function *induced by M with degree v.*

It can be seen in the proof of Zhang-Yeung, characterizing random vectors of matroidal entropy functions on $R_{U_{2,3}}$ is constructed by the multiplication table of an additive group on $\mathbb{Z}_v$. It is not difficult to see that a random vector constructed by any quasigroup on $\mathbb{Z}_v$, or equivalently, a Latin square with symbols in $\mathbb{Z}_v$, or equivalently, an orthogonal array $\mathrm{OA}(2, 3, v)$, characterizes $\log v \cdot U_{2,3}$. (See Section 2.2 for the definition of an orthogonal array.) More generally, an $\mathrm{OA}(t, n, v)$ can be used to construct a characterizing random vector of the matroidal entropy function $\log v \cdot U_{t,n}$ with $t \geq 2$. It is a natural question to ask whether such construction can be generalized to an arbitrary connected matroid M with rank ≥ 2? In [8], partition-representations $\xi_i, i \in N$ of a matroid $M = (N, \mathbf{r})$ with degree v was defined, where each ξ_i is partition of a set Ω with cardinality $v^{\mathbf{h}(N)}$. See more details in Sections 3.1.2. Characterizing random vectors of $\mathbf{h} = \log v \cdot \mathbf{r}$ can be obtained by the uniform distributions on the blocks of ξ_i. In [9], an equivalent definition in coding theory called almost affine code was defined. In this paper, in coordinate with the language in combinatorial design, we introduce variable strength orthogonal arrays(VOA) indexed by matroid M and integer $v \geq 2$, which is equivalent to a partition-representation of M with degree v and an (M, v) almost affine code. We denoted it by $\mathrm{VOA}(M, v)$. A $\mathrm{VOA}(M, v)$ can be regarded as expanding the concept of orthogonal array. If a $\mathrm{VOA}(M, v)$ exists, we will prove that the matroidal entropy function $\log v \cdot M$ is entropic and a characterizing random

vector of $\log v \cdot M$ can be constructed by VOA(M, v). On the other hand, if VOA(M, v) does not exist, $\log v \cdot M$ is non-entropic.

It is well known that orthogonal arrays with index unity in design theory are equivalent to maximum distance saperable (MDS) codes in coding theory. In discussions of our paper, we also see a more generalized equivalence, i.e., the equivalence between a VOA and an almost affine code. Thus, we review and develop the correspondences and equivalences in literatures such as [8,9] among four fields, i.e., information theory, matroid theory, combinatorial design, and coding theory, which may help them benefit from each other. In this paper, VOAs are also leveraged to characterize matroidal entropy functions induced by matroids of order $n \leq 5$.

The rest of this paper is organized as follows. Section 2 gives the preliminaries on matroid theory and orthogonal arrays. In Section 3, we first define variable strength orthogonal arrays and show their equivalence to the partition representation of a matroid and almost affine codes. Then we characterize matroid entropy functions via variable strength orthogonal arrays. in Section 4 , we characterize matroidal entropy functions of order $n \leq 5$. A discussion of the applications and further research is in Section 5.

2. Preliminary

2.1. Matroids

There exist various cryptomorphic definitions of a matroid. In this paper we discuss matroid theory mainly from the perspective of rank functions. For a detailed treatment of matroid theory, readers are referred to [10,11]. In Section 1, we defined matroids as special cases of polymatroids. Here we restate the definition in the following.

Definition 3. *A* matroid *M is an ordered pair $(N, \mathbf{r})$, where the* ground set *N is a finite set and the* rank function *$\mathbf{r}$ is a set function on 2^N, and they satisfy the conditions that: for any $A, B \subseteq N$,*

- $0 \leq \mathbf{r}(A) \leq |A|$ *and* $\mathbf{r}(A) \in \mathbb{Z}$,
- $\mathbf{r}(A) \leq \mathbf{r}(B)$, *if* $A \subseteq B$,
- $\mathbf{r}(A) + \mathbf{r}(B) \geq \mathbf{r}(A \cup B) + \mathbf{r}(A \cap B)$.

The value $\mathbf{r}(N)$ is called the rank *of M.*

With a slight abuse of terminology and notations, we do not distinguish a matroid and its rank function. So $M, \mathbf{r}_M$ and $\mathbf{r}$ may all denote the rank function of M when there is no ambiguity.

Definition 4. *For integer $n \geq 1$ and $0 \leq t \leq n$, the* uniform matroid *$U_{t,n}$ with rank t and order n is defined by*

$$U_{t,n}(A) := \min\{t, |A|\} \quad \forall A \subseteq N.$$

Given a matroid $M = (N, \mathbf{r})$, for $i \in N$, if $\mathbf{r}(i) = 0$, element i is called a loop of M. For $A \subseteq N$, if $\mathbf{r}(A) = 1$, we call A a parallel class. If $|A| \geq 2$, the parallel class is called non-trivial. A matroid is called simple if it contains no loops and no non-trivial classes. For a matroid M, if we delete its loops and in each non-trivial parallel class, we delete all elements but one, then we obtain a simple matroid M'. We call M' the simplification of M.

For a matroid $M = (N, \mathbf{r})$, a nonempty $C \subseteq N$ is called a circuit with size $|C|$ of M if $\mathbf{r}(C - x) = \mathbf{r}(C) = |C| - 1$ for any $x \in C$. It can be seen that any loop of M is a circuit of size 1 and a parallel pair $\{i, j\}$ is a circuit of size 2. For a uniform matroid $U_{t,n}$, circuits are exactly those $(t+1)$-subsets C of N. In particular, $U_{0,n}$ contains n loops, any two elements of $U_{1,n}$ are parallel, and the ground set of $U_{n-1,n}$ forms the unique circuit of $U_{n-1,n}$.

Definition 5. *A matroid is* connected *if any two elements in the ground set are contained in a circuit.*

It is easy to be verified that any uniform matroid $U_{t,n}$ with $1 \leq t \leq n-1$ is connected. This is because any $x \in N$ is contained in a $t+1$ subset of N which is a circuit of $U_{t,n}$.

An extreme ray R of a convex cone C is a subset of C and for any $\mathbf{r} \in R$ such that $\mathbf{r} = \mathbf{c}_1 + \mathbf{c}_2$ and $\mathbf{c}_1, \mathbf{c}_2 \in C$, we have $\mathbf{c}_1, \mathbf{c}_2 \in R$, where $\mathbf{c}_1 = a\mathbf{r}$ and $\mathbf{c}_2 = (1-a)\mathbf{r}$ for some $a \in \mathbb{R}$.

Lemma 1. *[12] A loopless matroid is connected if and only if M is contained in an extreme ray of Γ_n.*

Each extreme ray of Γ_n contains an integer-valued polymatroid, some of which are matroids. Such a matroid on an extreme ray is either a loopless connected matroid as stated in the above lemma, or a matroid obtained by adding loops to a connected matroids.

2.2. Orthogonal Arrays

Orthogonal array is a well studied topic in design theory. In this paper, orthogonal arrays are leveraged to characterize matroidal entropy functions. For a detailed treatment of this topic, readers are referred to [13].

Definition 6. *A $\lambda v^t \times n$ array T with entries from $\mathbb{Z}_v$ is called an* orthogonal array *of* strength *t,* factor *n,* level *v and* index *λ if for any $\lambda v^t \times t$ subarray T' of T, each t-tuple in $\mathbb{Z}_v^t$ occurs in the rows of T' exactly λ times. We call T an* $\mathrm{OA}(\lambda \times v^t; t, n, v)$. *When $\lambda = 1$, we say such orthogonal array has* index unity *and call it an* $\mathrm{OA}(t, n, v)$ *for short.*

By the definition, for any $1 \leq t' < t$, an $\mathrm{OA}(\lambda \times v^t; t, n, v)$ is also an $\mathrm{OA}(\lambda' \times v^{t'}; t', n, v)$, where $\lambda' = \lambda v^{t-t'}$. In this paper, we only consider the strength of the orthogonal array largest possible.

An important research problem of orthogonal arrays is the existence of an $\mathrm{OA}(t, n, v)$. The following lemmas state some results of this problem, in which Lemmas 2–4 can be found in Handbook [14].

Lemma 2 ([14], (III.7.16))**.** *There exists an* $\mathrm{OA}(t, t+1, v)$ *for any $v \in \mathbb{Z}^+$.*

Lemma 3 ([14], (III.3.28, III.3.39))**.** *For $v \in \mathbb{Z}^+$, an* $\mathrm{OA}(2, 4, v)$ *exists if and only if $v \neq 2, 6$.*

The nonexistence of $\mathrm{OA}(2, 4, 6)$ in Lemma 3 is the famous Euler's 36 officer problem.

Lemma 4 ([14], (III.3.28, III.3.36, III.3.39))**.** *An* $\mathrm{OA}(2, 5, v)$ *exists for all $v \in \mathbb{Z}^+$ with three exceptions $v = 2, 3, 6$ and one possible exception $v = 10$.*

Lemma 5. *For $v = 2, 3, 6$, there does not exist an* $\mathrm{OA}(3, 5, v)$.

This lemma is a folklore in the combinatorial design community. For self-contain, we prove it in the following.

Proof. We prove the non-existence of $\mathrm{OA}(3, 5, v)$ for $v = 2, 6$ by contradiction. Assume there exists an $\mathrm{OA}(3, 5, 2)$ $\mathbf{A}$, i.e., a $2^3 \times 5$ array whose each $2^3 \times 3$ subarray contains each 3-tuple in $\mathbb{Z}_2^3$ as a row exactly one time. By permuting the rows of $\mathbf{A}$, we obtain an $\mathrm{OA}(3, 5, 2)$ $\mathbf{A}'$ such that the entries in the first 2^2 rows and the 5-th column of $\mathbf{A}'$ are all 0. Let $\mathbf{c}_i, 1 \leq i \leq 5$ be the 5 columns of $\mathbf{A}'$ and $\mathbf{c}'_i$ be the vector consisting of the first 2^2 entries in $\mathbf{c}_i$. Now consider the subarray $[\mathbf{c}_i, \mathbf{c}_j, \mathbf{c}_5]$ with $1 \leq i < j \leq 4$. As its rows are exactly all 3-tuples in $\mathbb{Z}_2^3$ and $\mathbf{c}'_5$ is a zero vetor, it can be seen that the rows of $[\mathbf{c}'_i, \mathbf{c}'_j]$ are exactly all 2-tuples in $\mathbb{Z}_2^2$. Thus, $[\mathbf{c}'_1, \mathbf{c}'_2, \mathbf{c}'_3, \mathbf{c}'_4]$ forms an $\mathrm{OA}(2, 4, 2)$ which contradicts Lemma 3. The non-existence of $\mathrm{OA}(3, 5, 6)$ can be proved similarly.

For $\mathrm{OA}(3, 5, 3)$, assume such an array $\mathbf{B}$ exists. As each $3^3 \times 3$ subarray of $\mathbf{B}$ contains each 3-tuple in $\mathbb{Z}_3^3$ as a row exactly one time, for each two rows of the $3^3 = 27$ rows of $\mathbf{B}$,

their Hamming distance must be ≥ 3. Therefore, any two Hamming balls with center a row of **B** and radius 1 are disjoint. As there are 27 such Hamming balls with each size 11, there are at least $27 \times 11 = 297$ 5-tuples, which contradicts the fact that only $3^5 = 243$ 5-tuples exist. □

Lemma 6 ([15]). *If $v \geq 4$ and $v \not\equiv 2 \pmod 4$, then there is an* $\mathrm{OA}(3, 5, v)$.

Lemma 7 ([16]). *Let x be an arbitrary odd positive integer. Let g be an arbitrary positive integer whose prime power factors are all ≥ 7 such that $g \equiv 3 \pmod 4$. Then*

1. *there is an* $\mathrm{OA}(3, 5, v)$ *with $v = 35xg + 5$, if $x \equiv 1 \pmod 4$;*
2. *there is an* $\mathrm{OA}(3, 5, v)$ *with $v = 35xg + 7$, if $x \equiv 3 \pmod 4$.*

3. Characterizing Matroidal Entropy Functions via Voa

In this section, we introduce variable strength orthogonal arrays and then show that they are equivalent to partition-representations of a matroid and almost affine code. We then characterize matroidal entropy functions via variable strength orthogonal arrays.

3.1. Three Equivalent Definitions

3.1.1. Variable-Strength Orthogonal Array

Definition 7. *Given a loopless matroid $M = (N, \mathbf{r})$ with $\mathbf{r}(N) \geq 2$, a $v^{\mathbf{r}(N)} \times n$ array T with columns indexed by N, entries from $\mathbb{Z}_v$, is called a variable strength orthogonal array(VOA) induced by M with level v if for any $A \subseteq N$, $v^{\mathbf{r}(N)} \times |A|$ subarray of T consisting of columns indexed by A satisfy the following condition: each row of this subarray occurs $v^{\mathbf{r}(N)-\mathbf{r}(A)}$ times. We also call such T a* $\mathrm{VOA}(M, v)$.

It can be seen that for each $v^{\mathbf{r}(N)} \times |A|$ subarray T' of T, $v^{\mathbf{r}(A)}$ distinct $|A|$-tuples in $\mathbb{Z}_v^{|A|}$ occur in T'. When A is independent, i.e., $\mathbf{r}(A) = |A|$, they are exactly all tuples in $\mathbb{Z}_v^{|A|}$.

Example 1. *Let $M_1 = (N, \mathbf{r}_1)$ be a matroid with $N = \{1, 2, 3, 4, 5\}$ and rank function*

$$\mathbf{r}_1(A) = \begin{cases} |A| & |A| \leq 2 \\ 2 & A \in \{\{1, 2, 3\}, \{3, 4, 5\}\} \\ 3 & o.w. \end{cases}$$

Then

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{array}$$

is a $\mathrm{VOA}(M_1, 2)$.

For a matroid M, let $\mathcal{C}$ be the set of all its circuits. From the definition, it can be seen that a $\mathrm{VOA}(M, v)$ is an $\mathrm{OA}(v^{\mathbf{r}(N)}; t, n, v)$ with $t = \min_{C \in \mathcal{C}} |C| - 1$, and so it has index $\lambda = v^{\mathbf{r}(N)-t}$. For the matroid M_1 in Example 1, as $\mathbf{r}(N) = 3$ and smallest circuits $\{1, 2, 3\}$ and $\{3, 4, 5\}$ have size 3, the $\mathrm{VOA}(M, v)$ is an $\mathrm{OA}(8; 2, 5, 2)$ and index $\lambda = 2$.

However, on the other hand, two $\mathrm{OA}(\lambda v^t; t, n, v)$s may be VOAs induced by two distinct matroids as long as they have the same rank and the same size of the smallest circuit. This is because the rank of a matroid provides richer parameters in VOA description than strength and index in OA description. The VOA description provides accurate information

on the vary of strength on different set of columns of the array. This is why we term it "variable strength orthogonal array".

Example 2. *Let* $M_2 = (N, \mathbf{r}_2)$ *be a matroid with* $N = \{1,2,3,4,5\}$ *and rank function*

$$\mathbf{r}_2(A) = \begin{cases} 2 & A = \{1,2,3\} \\ |A| & |A| < 3 \\ 3 & o.w. \end{cases}$$

Then VOA(M_1, v) *and* VOA(M_2, v) *are both* OA$(v^3; 2, 5, v)$.

However, when the matroid is uniform, the two descriptions are equivalent. For a uniform matroid $U_{t,n}$, as any circuit has size $t+1$, a VOA$(U_{t,n}, v)$ has strength t and index $\lambda = 1$, i.e., an OA(t, n, v). On the other hand, it can be seen any OA(t, n, v) is a VOA$(U_{t,n}, v)$. So in the following of this paper, we write VOA$(U_{t,n}, v)$ as OA(t, n, v) for simplicity.

3.1.2. Partition-Representation of A Matroid

We will see that a partition-representation of a matroid M with degree v defined in [8] is equivalent to an VOA(M, v).

Definition 8. *Let* $M = (N, \mathbf{r})$ *be a matroid with ground set* N *and rank function* $\mathbf{r}$. *Let* $v \in \mathbb{Z}^+$. *The matroid* M *is partition representable of degree* v *if there exist a finite set* Ω *of cardinality* $v^{\mathbf{r}(N)}$ *and partitions* ξ_i *of* Ω, $i \in N$, *such that for any* $A \subseteq N$, *the meet-partition* $\xi_A = \wedge_{i \in A} \xi_i$ *has* $v^{\mathbf{r}(A)}$ *blocks all the same cardinality.*

Let Ω be the set of all rows of an VOA(M, v). Let ξ_i be a partition of Ω such that the rows in each block of ξ_i have the same entry in the i-th column. It can be seem that $\xi_i, i \in N$ is a partition-representation of M with degree v.

On the other hand, let $\xi_i, i \in N$, be a partition-representation of a loopless matroid M with degree v, living on Ω. As each ξ_i has v blocks, we label them from 0 to $v-1$. Now for each $\mathbf{x} \in \Omega$, it is labelled by an $|N|$-tuple $(x_i, i \in N)$ where x_i is the label of the block of ξ_i to which $\mathbf{x}$ belong. Let A be an array whose rows are exactly the labels of all $\mathbf{x} \in \Omega$. It can be checked that A is an VOA(M, v).

3.1.3. Almost Affine Codes

Almost affine codes were introduced in [9]. For vector space $\mathbb{F}_q^N$ over finite field $\mathbb{F}_q$, where q is a prime power, a linear subspace of $\mathbb{F}_q^N$ forms a linear code of length n, while each coset of a linear code are called an affine code. For an affine code $\mathcal{C} \subset \mathbb{F}_q^N$ and any $A \subseteq N$, let $\mathcal{C}_A$ be the projection of $\mathcal{C}$ onto $\mathbb{F}_q^A$, it can be seen that $|\mathcal{C}_A|$ is a power of q. But there are other codes satisfy this property even if they are not codes over a finite fields.

Definition 9. *For a set of* v *symbols, say* $\mathbb{Z}_v$, $\mathcal{C} \subseteq \mathbb{Z}_v^N$ *is called an* almost affine code *if*

$$\mathbf{r}(A) := \log_v |\mathcal{C}_A| \tag{1}$$

is an integer for all $A \subseteq N$.

For any almost affine code $\mathcal{C}$, $(N, \mathbf{r})$ forms a matroid M, where the rank function $\mathbf{r}$ is defined in (1). We call such almost affine code an (M, v) (almost affine) code.

For an (M, v) code, if M is a uniform matroid $U_{t,n}$, it coincides with an (n, t, v) maximum distance separable (MDS) code.

By checking the definition of a VOA(M, v) and an (M, v) almost affine code, it can be seen that rows of a VOA(M, v) are exactly codewords of an (M, v) almost affine code and

vice versa. In particular, the rows of a $\mathrm{OA}(t, n, v)$ are exactly codewords of an (n, t, v)-MDS code and vice versa.

If there exists an (M, v) almost affine code, M is called almost affinely representable with degree v.

3.2. Characterizing Matroidal Entropy Functions via VOA

Given a random vector (X_i, N), let $p_{X_N}(\cdot)$ denote its joint probability mass function, and for any $A \subseteq N$, $p_{X_A}(\cdot)$ be the marginal distribution function on A. Without loss of generality, we assume each random variable X_i is distributed on $\mathbb{Z}_{v_i}$ and for each $x \in \mathbb{Z}_{v_i}$, $p_{X_i}(x) > 0$.

Theorem 1. *A random vector* $\mathbf{X} = (X_i : i \in N)$ *characterizes the matroidal entropy function* $\log v \cdot M$ *for a connected matroid* $M = (N, \mathbf{r})$ *with rank* $\mathbf{r}(N) \geq 2$ *if and only if the random variable* $\mathbf{X}$ *is uniformly distributed on the rows of a* $\mathrm{VOA}(M, v)$.

Proof. Given a $\mathrm{VOA}(M, v)$, randomly pick a row from it according to the uniform distribution. Let $X_i, i \in N$, be the random variable of i-th entries of picked n-tuple. For any $A \subseteq N$, consider the $v^{\mathbf{r}(N)} \times |A|$ subarray of the $\mathrm{VOA}(M, v)$ consisting of columns indexed by A. By definition, it contains $v^{\mathbf{r}(A)}$ $|A|$-tuples in $\mathbb{Z}_v^{|A|}$ as rows with each $v^{\mathbf{r}(N)-\mathbf{r}(A)}$ times. Hence $\mathbf{h}_{\mathbf{X}}(A) = \log v \cdot \mathbf{r}(A)$. It proves that $\mathbf{X}$ characterizes $\log v \cdot M$ and thus the "if part" of the theorem.

For the "only if part", let $\mathbf{X} = (X_i : i \in N)$ be a characterizing random vector of $\log v \cdot M$. Take $C \subseteq N$ be a circuit of M of with cardinality $n' \geq 3$. WLOG, we asume $C = \{1, 2, \cdots, n'\}$. Then for each $A \subsetneq C$, $X_i, i \in A$ are mutually independent, and for each $i \in C$, X_i is a function of $(X_j : j \in C - i)$. Then for each $A \subsetneq C$ and $x_i \in \mathbb{Z}_{v_i}, i \in A$, $p_{X_A}(x_i : i \in A) = \prod_{i \in A} p_{X_i}(x_i)$, and for each $i \in C$, $p_{X_C}(x_j : j \in C) = p_{X_{C-i}}(x_j : j \in C - i)$. In particular,

$$p_{X_C}(x_1, x_2 \cdots, x_{n'}) = p_{X_{C-1}}(x_2, \cdots, x_{n'}) = p_{X_2}(x_2) ... p_{X_{n'}}(x_{n'}) \tag{2}$$

and

$$p_{X_C}(x_1, x_2 \cdots, x_{n'}) = p_{X_{C-2}}(x_1, x_3 \cdots, x_{n'}) = p_{X_1}(x_1) p_{X_3}(x_3) ... p_{X_{n'}}(x_{n'}) \tag{3}$$

Equating (2) and (3), we have

$$p_{X_1}(x_1) = p_{X_2}(x_2). \tag{4}$$

Let $x_1' \in \mathcal{X}_1$ and $x_1' \neq x_1$, with the same argument, we have

$$p_{X_1}(x_1') = p_{X_2}(x_2). \tag{5}$$

As x_1 and x_1' are arbitrary chosen from $\mathbb{Z}_{v_1}$, X_1 is uniformly distributed on it. Since $\mathbf{h}_{\mathbf{x}}(\{1\}) = \log v$, $v_1 = v$. By symmetry, for all $i \in C$, X_i is uniformly distributed on $\mathbb{Z}_v$. Since M is a connected matroid with $\mathbf{r}(N) \geq 2$, each element is contained in a circuit with size not less than 3. Hence for all $i \in N$, X_i is uniformly distributed on $\mathbb{Z}_v$. Thus, in the following $\mathbf{X}$ can be considered to distributed on $\mathbb{Z}_v^N$ and for any $A \subseteq N$, X_A is distributed on $\mathbb{Z}_v^A$.

Now let $B \subseteq N$ be a base of M, i.e., $\mathbf{r}(B) = |B| = \mathbf{r}(N)$. Since $\mathbf{h}_{\mathbf{X}}(B) = \log v \cdot \mathbf{r}(N)$, any $|B|$-tuple $\mathbf{x}_B$ in $\mathbb{Z}_v^B$, $p_{X_B}(\mathbf{x}_B) = v^{-\mathbf{r}(N)} > 0$. It implies that there exists at least $v^{\mathbf{r}(N)}$ n-tuples $\mathbf{x} \in \mathbb{Z}_v^N$ with $p_N(\mathbf{x}) > 0$ and the marginal distribution of them on B is uniform. As $\mathbf{h}_{\mathbf{X}}(N) = \mathbf{h}_{\mathbf{X}}(B) = \log v \cdot \mathbf{r}(N)$, each $\mathbf{x} \in \mathbb{Z}_v^N$ with $p_N(\mathbf{x}) > 0$ is uniquely determined by their entries indexed by B, and so there are exactly $v^{\mathbf{r}(N)}$ n-tuples $\mathbf{x} \in \mathbb{Z}_v^N$ with $p_N(\mathbf{x}) = v^{-\mathbf{r}(N)}$ and other n-tuples has zero probability. Furthermore, for any $A \subseteq N$, as $\mathbf{h}_{\mathbf{X}}(A) = \log v \cdot \mathbf{r}(A)$, by taking sub-tuples indexed by A of these $v^{\mathbf{r}(N)}$ n-tuples, we obtain $v^{\mathbf{r}(A)}$ distinct $|A|$-tuple in $\mathbb{Z}_v^{|A|}$, each of which occur exactly $v^{\mathbf{r}(N)-\mathbf{r}(A)}$ times. Therefore, if we put these n-tuples in an array and each as a row, they form a $\mathrm{VOA}(M, v)$. □

Corollary 1. *A random vector* $\mathbf{X} = (X_i : i \in N)$ *characterizes matroidal entropy function* $\log v \cdot U_{t,n}$ *with* $2 \le t \le n-1$ *if and only if random variable* $Y = \mathbf{X}$ *is uniformly distributed on the rows of an* $\mathrm{OA}(t, n, v)$.

4. P-Characteristic Set of Matroids with Order $n \le 5$

Rank 1 matroids of order n are exactly those matroids containing $U_{1,n'}$ on $N' \subseteq N$ as a submatroid and other elements loops. Let X be an arbitrary random variable. Let $(X_i : i \in N)$ be defined by

$$X_i = \begin{cases} X & i \in N' \\ \text{a constant.} & \text{o.w.} \end{cases}$$

It can be seen that $(X_i : i \in N)$ characterizes $\mathbf{h}$ on the ray $\{\mathbf{h} \in \mathcal{H}_n : \mathbf{h} = c \cdot M\}$ as long as we let $H(X) = c$.

Armed with the results of orthogonal arrays in Section 2.2 and Theorem 1, we can characterize the matroidal entropy functions $\log v \cdot M$ for a connected matroid M with rank ≥ 2. In this section, we determine the p-characteristic set χ_M for all connected matroids $M = (N, \mathbf{r})$ with rank $\mathbf{r}(N) \ge 2$ and order $n \le 5$. For a disconnected matroid M with each connected component M_i rank ≥ 2, χ_M is the intersections of all χ_{M_i}. Thus, it is sufficient to consider connected matroids and take them as building blocks. It matches the fact that matroidal entropy functions indexed by a connected matroid live on an extreme rays of Γ_n (see Lemma 1), while those indexed by a disconnected matroid can be written as the sum of the matroidal entropy functions indexed by its connected components.

Among all connected matroids, we only need to consider those simple matroids since the p-characteristic set of a matroid is the same as its simplification. For a matroid $M = (N, \mathbf{r})$ and its simplification $M' = (N', \mathbf{r}')$ with $N' \subseteq N$, if $(Y_j : j \in N')$ characterizes $\log v \cdot M'$, for each parallel class A, let $X_i = Y_j : i \in A$ where j is the only element in $A \cap N'$, and let X_i be a constant if i is a loop of M. Then $(X_i : i \in N)$ characterizes $\log v \cdot M$. On the other hand, if $(X_i : i \in N)$ characterizes $\log v \cdot M$, by the reverse method, we obtain $(Y_j : j \in N')$ characterizing M'. Hence they have the same p-characteristic set.

Non-isomorphic simple matroids with order ≤ 8 is listed in [17] (A simple matroid is also called a combinatorial geometry.). Here we consider connected simple matroids with rank $\mathbf{r}(N) \ge 2$ and order $n \le 5$. Before that we first consider $U_{n-1,n}$ for general $n \ge 3$. By Lemma 2 and Theorem 1, we have the following proposition.

Proposition 1.

$$\chi_{U_{n-1,n}} = \{v \in \mathbb{Z} : v \ge 2\}.$$

When $n = 3$, the case $U_{2,3}$ is also proved by Zhang-Yeung [1] as we discussed in Section 1. As $U_{2,3}$ is the only case we need to consider for matroids with oder $n = 3$, in the following we discuss the cases for $n = 4$ and 5.

4.1. $n = 4$

For $n = 4$, besides $U_{3,4}$, one more matroid we need to consider is $U_{2,4}$. By Theorem 1 together and Lemma 3, we have the following propositions.

Proposition 2.

$$\chi_{U_{2,4}} = \{v \in \mathbb{Z} : v \ge 3, v \ne 6\}.$$

4.2. $n = 5$

For $n = 5$, besides $U_{4,5}$, there are four more matroids we need to consider, namely, $U_{2,5}$, $U_{3,5}$, M_1 defined in Example 1 and M_2 defined in Example 2.

For $U_{2,5}$, by Theorem 1 and Lemma 4, we have the following propositions.

Proposition 3. *For* $U_{2,5}$, $2, 3, 6 \notin \chi_{U_{2,5}}$ *and* $\mathbb{Z}^+ \setminus \{2, 3, 6, 10\} \subseteq \chi_{U_{2,5}}$.

For $U_{3,5}$, by Theorem 1 and Lemmas 5–7, we have the following propositions.

Proposition 4. *For $U_{3,5}$, $2,3,6 \notin \chi_{U_{3,5}}$ and $V \subseteq \chi_{U_{2,5}}$, where $V = V_1 \cup V_2$ and*

1. $V_1 = \{v \geq 4 : v \not\equiv 2 \pmod 4\}$
2. *V_2 is the set of $v \equiv 2 \pmod 4$ such that*
   - $v = 35xg + 5$, *if* $x \equiv 1 \pmod 4$;
   - $v = 35xg + 7$, *if* $x \equiv 3 \pmod 4$

   where x is an arbitrary odd positive integer, and g is an arbitrary positive integer whose prime power factors are all ≥ 7 such that $g \equiv 3 \pmod 4$.

For M_1, we give a VOA$(M_1, 2)$ in Example 1, thus $2 \in \chi_{M_1}$. We will have in the following proposition on the existence of VOA(M_1, v) for an arbitrary $v \geq 2$.

Proposition 5.

$$\chi_{M_1} = \{v \in \mathbb{Z} : v \geq 2\}.$$

Proof. For any $v \geq 2$, let (y_1, y_2, y_3) be any 3-tuple in $\mathbb{Z}_v^3$. Now given (y_1, y_2, y_3), let $x_1 = y_1$, $x_2 = y_2$, $x_3 = y_1 + y_2$, $x_4 = y_3$ and $x_5 = x_1 + x_2 + x_3$, we obtain a 5-tuple $(x_1, x_2, x_3, x_4, x_5)$. Run out of all $(y_1, y_2, y_3) \in \mathbb{Z}_v^3$, it can be checked that the resulting v^3 5-tuples form a VOA(M, v). Since $v \geq 2$ is arbitrary, the proposition holds. □

The following proposition determines the p-characteristic set of M_2

Proposition 6.

$$\chi_{M_2} = \{v \in \mathbb{Z} : v \geq 3, v \neq 6\}.$$

Proof. We prove that if there exist an OA$(2, 4, v)$, then there exists a VOA(M_2, v), and vice versa. It implies that $\chi_{M_2} = \chi_{U_{2,4}}$ and hence the proposition.

Now assume there is an OA$(2, 4, v)$ with columns $\mathbf{a}_i, i = 1, 2, 3, 4$. So each $\mathbf{a}_i$ is a v^2-vector. Let $\mathbf{b}_i, i = 1, 2, 3, 4, 5$ be v^3-vectors defined as follows.

$$\mathbf{b}_i(kv^2 + j) = \begin{cases} \mathbf{a}_i(j) & i = 1, 2, 3 \\ \mathbf{a}_4(j) + k \bmod v & i = 4 \\ k & i = 5 \end{cases}$$

for each $j = 1, 2, \cdots, v^2$ and $k = 0, 1, \cdots, v - 1$. It can be checked that $\mathbf{b}_i, i = 1, 2, 3, 4, 5$ form a VOA(M_2, v).

On the other hand, assume there is a VOA(M_2, v) with columns $\mathbf{b}_i, i = 1, 2, 3, 4, 5$. As $\mathbf{r}(\{5\}) = 1$ and $\mathbf{r}(N) = 3$. The fifth column of VOA(M_2, v) contains each $i \in \mathbb{Z}_v$ v^2 times. Rearrange the rows of VOA(M_2, v) such that the first v^2 entries of $\mathbf{b}_5$ are zeros, i.e., $\mathbf{b}_5(j) = 0$ for $j = 1, 2, \cdots, v^2$. Let $\mathbf{a}_i = 1, 2, 3, 4$ be v^2-vectors and $\mathbf{a}_i(j) = \mathbf{b}_i(j)$ for $j = 1, 2, \cdots, v^2$. Then it can be checked that $\mathbf{a}_i = 1, 2, 3, 4$ form an OA$(2, 4, v)$. □

5. Discussion

5.1. Applications

Matroidal entropy functions and its characterizations have many potential applications in information theory. In the following we discuss the applications to network coding and secret sharing.

5.1.1. Network Coding

A method of building networks from matroids was given in [18]. In a matroidal network G, messages generated in the source nodes and transmitted on the edges are mapped to the ground set of a matroid M (See Section V.B of [18]). By the same mapping, a

VOA(M, v) with $v \geq 2$ can be considered as a $(1, 1)$ coding solution with alphabet size v of the network G. This coding solution is scalar but may not need to be linear.

5.1.2. Secret Sharing

Let M be a connected matroid with rank ≥ 2 and N be its ground set. Let $1 \in N$ be the special element. Let $\mathcal{A}_{\mathrm{m}} = \{C \setminus \{1\} : 1 \in C, C \text{ is a circuit of } M\}$ and $\mathcal{A} = \{A \subseteq N : \exists B \in \mathcal{A}_{\mathrm{m}} \text{ s.t. } B \subseteq A\}$. It can the checked that a VOA(M, v) forms an ideal secret sharing scheme of the access structure $\mathcal{A}$, where the dealer is indexed by 1 and other participants are indexed by $x \in N \setminus \{1\}$. Such constructions can be seen in literatures such as [19–23].

5.2. Further Research

In this paper, we review and developed correspondences among matroidal entropy functions, connected matroids with rank ≥ 2, variable strength orthogonal arrays and almost affine codes. These correspondences can make them benefit from each other, and therefore yield more research topics in the following facets.

1. Results of orthogonal arrays can be leveraged to characterize matroidal entropy functions as we do in Section 4 for those of order ≤ 5.
2. Abundant tools in matroid theory can be used to study matroidal entropy functions, VOAs and almost affine codes. For example, in the proof of Lemma 5 and Proposition 6 , we implicitly use the fact that $U_{2,4}$ is minor of $U_{2,5}$ and M_2, and $U_{2,4}$ is a forbidden minor for characteristic 2 and 6.
3. Matroid representability is an important and well-studied area in matroid theory. See [11], (Chapter 6). A matroid $M = (N, \mathbf{r})$ is called representable over a field $\mathbb{F}$ if there exists a matrix T with entries in $\mathbb{F}$ whose columns are indexed by N, and for each $A \subseteq N$, the rank of the submatrix consisting of the columns indexed by A is equal to $\mathbf{r}(A)$. As we discussed in Section 3.1.2 and 3.1.3, a matroid is called partition-representable [8] or almost affinely representable [9] with degree v if there exists a VOA(M, v). Obviously, an $\mathbb{F}_q$-representable matroid is also partition-representable with degree q. However, the converse of the statement may not hold in general.
4. The construction of an OA(t, n, v) is also an important problem in combinatorial design. For some parameters, say OA$(2, 5, 10)$, the problem is extremely difficult. The definition of VOA provides more tools to attack the problem.
5. Matroidal entropy functions induced by $U_{t,n}$ are called symmetric matroidal entropy functions. They are special cases of the p-symmetrical entropy functions, where p is the trivial partition of N with N being the only block. In general, for an arbitrary permutation group G on N, symmetries of an G-symmetric matroidal entropy function, i.e., an entropy function that is G-symmetric [24] and matroidal, can be utilized to construct its characterizing random vectors via VOA. [25].

Author Contributions: Conceptualization, Q.C. and M.C.; methodology, Q.C., M.C. and B.B.; writing—original draft preparation, Q.C.; writing—review and editing, Q.C., M.C. and B.B. All authors have read and agreed to the published version of the manuscript.

Funding: Please add: Qi Chen is sported by NSFC61971321 and the Fundamental Research Funds for the Central Universities. Minquan Cheng is supported by Guangxi Collaborative Innovation Center of Multi-source Information Integration and Intelligent Processing, the Guangxi Bagui Scholar Teams for Innovation and Research Project, and the Guangxi Talent Highland Project of Big Data Intelligence and Application. Baoming Bai is supported by the Key Research and Development Project of Guangdong Province under Grant 2018B010114001.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank four reviewers for their valuable comments that make this paper more readable. Then the authors thank Guangzhou Chen for his introduction of the results on

orthogonal arrays. Finally the authors thank IEEE Information Theory Society Guangzhou Chapter for proposing opportunities to discuss the results of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

OA	Orthogonal array
VOA	variable strength orthogonal array
MDS	Maximum distance separable
WLOG	With loss of generality

References

1. Zhang, Z.; Yeung, R.W. A non-Shannon type conditional inequality of information quantities. *IEEE Trans. Inf. Theory* **1997**, *43*, 1982–1986. [CrossRef]
2. Fujishige, S. Polymatroidal dependence structure of a set of random variables. *Inf. Contr.* **1978**, *39*, 55–72. [CrossRef]
3. Yeung, R.W. *Information Theory and Network Coding*; Springer: Berlin/Heidelberg, Germany, 2008.
4. Yeung, R.W. Facets of entropy. *IEEE Inf. Theory Soc.* **2012**, **62(8)**, 6–15. [CrossRef]
5. Chan, T. Recent progresses in characterizing information inequalities. *Entropy* **2011**, *13*, 379–401. [CrossRef]
6. Zhang, Z.; Yeung, R.W. On characterization of entropy function via information inequalities. *IEEE Trans. Inf. Theory* **1998**, *44*, 1440–1452. [CrossRef]
7. Matúš, F. Probabilistic conditional independence structures and matroid theory: Background. *Int. J. Gen. Syst.* **1994**, *22*, 185–196. [CrossRef]
8. Matúš, F. Matroid representations by partitions. *Discrete Math.* **1999**, *203*, 169–194. [CrossRef]
9. Simonis, J.; Ashikhmin, A. Almost affine codes. *Desings Codes Cryptogr.* **1998**, *14*, 179–797. [CrossRef]
10. Welsh, D.J.A. *Matroid Theory*; Academic Press: Cambridge, MA, USA, 1976.
11. Oxley, J.G. *Matroid Theory*; Oxford Univ. Press: Oxford, UK, 1992.
12. Nguyen, H.Q. Semimodular functions and combinatorial geometries. *Trans. AMS* **1978**, *238*, 355–383. [CrossRef]
13. Hedayat, A.S.; Sloane, N.J.A.; Stufken, J. *Orthogonal Arrays: Theory and Applications*; Springer: New York, NY, USA, 1999.
14. Colbourn, C.J.; Dinitz, J.H. *Handbook of Combinatorial Designs*; CRC Press: Boca Raton, FL, USA, 2007.
15. Ji, L.; Yin, J. Constructions of new orthogonal arrays and covering arrays of strength three. *J. Comb. Theory Ser. A* **2010**, *117*, 236–247. [CrossRef]
16. Yin, J.; Wang, J.; Ji, L.; Li, Y. On the existence of orthogonal arrays $\mathrm{OA}(3,5,4n+2)$. *J. Comb. Theory Ser. A* **2011**, *118*, 270–276. [CrossRef]
17. Blackburn, J.E.; Crapo, H.H.; Higgs, D.A. A catalogue of combinatorial geometries. *Math. Comp.* **1973**, *27*, 155–166. [CrossRef]
18. Dougherty, R.; Freiling, C.; Zeger, K. Networks, Matroids, and non-Shannon Information Inequalities. *IEEE Trans. Inf. Theory* **2007**, *53*, 1949–1969. [CrossRef]
19. Brickell, E.F.; Davenport, D.M. On the classification of ideal secret sharing schemes. *J. Cryptol.* **1991**, *4*, 123–134. [CrossRef]
20. Golic, J.D. On matroid characterization of ideal secret sharing schemes. *J. Cryptol.* **1998**, *11*, 75–86. [CrossRef]
21. Blakley, G.R.; Kabatianski, G.A. General Perfect Secret Sharing Schemes. In Proceedings of the CRYPTO '95: 15th Annual International Cryptology Conference, Santa Barbara, CA, USA, 27–31 August 1995; Volume 963, pp. 367–371.
22. Ng, S.-L. A representation of a family of secret sharing matroids. *Des. Codes Cryptogr.* **2003**, *30*, 5–19. [CrossRef]
23. Martí-Farré, J.; Padró, C. Secret sharing schemes with three or four minimal qualified subsets. *Des. Codes Cryptogr.* **2005**, *34*, 17–34. [CrossRef]
24. Apte, J.; Chen, Q.; Walsh, J.M. Symmetries in the Entropy Space. In Proceedings of the IEEE Information Theory Workshop, Cambridge, UK, 11–14 September 2016.
25. Chen, Q.; Yeung, R.W. Partition-Symmetrical Entropy Functions. *IEEE Trans. Inf. Theory* **2016**, *62*, 5385–5402. [CrossRef]