Article

Entropy of Closure Operators and Network Coding Solvability

Maximilien Gadouleau

School of Engineering and Computing Sciences, Durham University, South Road, DH1 3LE, Durham, UK; E-Mail: m.r.gadouleau@durham.ac.uk

Abstract: The entropy of a closure operator has been recently proposed for the study of network coding and secret sharing. In this paper, we study closure operators in relation to their entropy. We first introduce four different kinds of rank functions for a given closure operator, which determine bounds on the entropy of that operator. This yields new axioms for matroids based on their closure operators. We also determine necessary conditions for a large class of closure operators to be solvable. We then define the Shannon entropy of a closure operator and use it to prove that the set of closure entropies is dense. Finally, we justify why we focus on the solvability of closure operators only.

Keywords: closure operators; entropy; network coding; information inequalities

1. Introduction

Network coding is a novel means to transmit data through a network, where each intermediate node determines its output packet from all of the packets it receives [1]. Network coding problems are further defined by restrictions on the alphabet of packets and sometimes on what computations the intermediate nodes may do. In particular, linear network coding [2] is optimal in the case of one source; however, this is not the case for multiple sources and destinations [3,4]. Although for large dynamic networks, good heuristics, such as random linear network coding [5,6], can be used, maximizing the amount of information that can be transmitted over a static network is fundamental, but very hard in practice. Solving this problem by brute force, *i.e.*, considering all possible operations at all nodes, is computationally prohibitive. The network coding solvability problem is given as follows: given a network (with corresponding graph, sources, destinations and messages), can all of the messages be transmitted? This problem is very difficult, for instance the problem for some networks is as hard as determining whether k mutually orthogonal Latin squares of order A exist [7,8].

Several major advances have been made on this problem. First of all, it can always be reduced to a multiple unicast instance, where each source sends a different message, requested to a corresponding unique destination. In [9], the network coding solvability problem is reduced to the guessing game (described in Section 2.4 below), a simple cooperative problem on arbitrary directed graphs, thus removing the asymmetry between sources, intermediate nodes and destinations. Notably, [10] introduces the entropy of a directed graph (not to be mistaken with Körner's graph entropy in [11] or with the Shannon capacity of a graph [12]); calculating this entropy solves the network solvability problem. This problem can be tackled by a more combinatorial approach, based on the so-called guessing number of a graph, which is closely related to the entropy [10]. The guessing number of graphs is studied further in [13], where it is proved that the guessing number of a directed graph is equal to the independence number of a related undirected graph. The guessing number of undirected graphs is further explored in [14].

A closure operator on the vertex set of a digraph is introduced in [8]. Network coding solvability is then proven to be a special case of a more general problem, called the closure solvability problem, for the closure operator defined on a digraph related to the network coding instance. The latter problem also generalises the search for ideal secret sharing schemes [15]. The main interest of closure solvability is that it allows us to use closure operators, which do not arise from digraphs (notably the uniform matroids), but which have been proven to be solvable over many alphabets. In this paper, we introduce the concept of the entropy of an arbitrary closure operator. Again, calculating the entropy of a closure operator determines whether this closure operator is solvable or not. Therefore, this paper aims at studying this quantity in detail.

The closure solvability problem generalises different problems in coding theory, cryptology or combinatorics.

- As mentioned above, closure operators associated with digraphs are particularly relevant for network coding. Indeed, a network coding instance is solvable if and only if cl_D is solvable for some digraph D related to the network coding instance [8].

- When reduced to matroids, this is the problem of representation by partitions in [16], which is equivalent to determining secret-sharing matroids [15].

- When further reduced to the uniform matroid, this is exactly the problem of finding maximum distance separable (MDS) codes, which is arguably the most important open problem in coding theory (see [17]). Special cases include the famous combinatorial problem of the existence of mutually orthogonal Latin squares.

The rest of the paper is organised as follows. We review the closure operator associated with a digraph and the general closure solvability problem in Section 2. In Section 3, we introduce four kinds of rank functions for a given closure operator. This not only helps us derive bounds on the entropy, but we are also able to provide axioms for matroids that are, to the author's knowledge, new. Section 4 then studies a natural upper bound on the entropy, based on polymatroids. This helps us prove that the set of closure entropies contains all rational numbers above one. Finally, Section 5 investigates the solvability problem beyond closure operators.

2. Preliminaries

2.1. Closure Operators

Throughout this paper, V is a set of n elements. A closure operator on V is a mapping $\mathrm{cl} : 2^V \to 2^V$, which satisfies the following properties (see Chapter IV in [18]). For any $X, Y \subseteq V$,

(1) $X \subseteq \mathrm{cl}(X)$ (extensive);

(2) if $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$ (isotone);

(3) $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ (idempotent).

A closed set is a set equal to its closure. For instance, in a group, one may define the closure of a set as the subgroup generated by the elements of the set; the family of closed sets is simply the family of all subgroups of the group. Another example is given by linear spaces, where the closure of a set of vectors is the subspace they span. Closure operators are central in lattice theory and in universal algebra; moreover, any Galois connection between subset lattices is equivalent to a closure operator on subsets.

We refer to:

$$r := \min\{|b| : \mathrm{cl}(b) = V\}$$

as the rank of the closure operator. Any set $b \subseteq V$ of size r and whose closure is V is referred to as a basis of cl. There is a natural partial order on closure operators of the same set. We denote $\mathrm{cl}_1 \leq \mathrm{cl}_2$ if for all $X \subseteq V$, $\mathrm{cl}_1(X) \subseteq \mathrm{cl}_2(X)$; then $r(\mathrm{cl}_1) \geq r(\mathrm{cl}_2)$.

We shall focus on two families of closure operators. Firstly, a matroid closure is a closure operator satisfying the Steinitz–Mac Lane exchange property (in order to simplify notation, we shall identify a singleton $\{v\}$ with its element v): if $X \subseteq V$, $v \in V$ and $u \in \mathrm{cl}(X \cup v) \backslash \mathrm{cl}(X)$, then $v \in \mathrm{cl}(X \cup u)$ [19]. In particular, the uniform matroid $U_{r,n}$ of rank r over n vertices is defined by:

$$U_{r,n}(X) = \begin{cases} V & \text{if } |X| \geq r \\ X & \text{otherwise.} \end{cases}$$

It is worth noting that matroids constitute a much richer variety than uniform matroids.

Secondly, let $D = (V, E)$ be a digraph on n vertices (possibly with loops, but without any repeated arcs). The in-neighborhood of a vertex v is denoted as $v^- = \{u : (u, v) \in E\}$; we extend this definition to subsets of vertices $Y^- = \bigcup_{v \in Y} v^-$. The D-closure of any $X \subseteq V$ is defined as follows [8]. We let $c_D(X) := X \cup \{v \in V : v^- \subseteq X\}$ and the D-closure of X is obtained by applying it c_D repeatedly n times: $\mathrm{cl}_D(X) := c_D^n(X)$.

This definition can be intuitively explained as follows. Suppose we assign a function to each vertex of D, which only depends on its in-neighbourhood (the function that decides which message the vertex will transmit). If we know the messages sent by the vertices of X, we also know the messages that will be sent by any vertex in $c_D(X)$. By applying this iteratively, we can determine all messages sent by the vertices in $\mathrm{cl}_D(X)$. Therefore, $\mathrm{cl}_D(X)$ represents everything that is determined by X.

Alternatively, we have $\mathrm{cl}_D(X) := X \cup Y$, where Y is the largest acyclic set of vertices, such that $Y^- \subseteq X \cup Y$ (see Lemma 1 in [8]). Recall that a feedback vertex set is a set of vertices X, such that

$V \backslash X$ induces an acyclic subgraph. The rank of cl_D is therefore the minimum size of a feedback vertex set of D.

Example 1. *The D-closure of some classes of graphs can be readily determined.*

(1) If D is acyclic, then $\mathrm{cl}_D = U_{0,n}$.

(2) If $D = C_n$, the directed cycle, then $\mathrm{cl}_D = U_{1,n}$.

(3) If $D = K_n$, the complete graph, then $\mathrm{cl}_D = U_{n-1,n}$.

(4) If D has a loop on each vertex, then $\mathrm{cl}_D = U_{n,n}$.

Conversely, no other uniform matroid can be viewed as a D-closure.

However, the following two questions are still open. For which digraphs are the D-closures matroids? What matroids are represented by D-closures of digraphs?

2.2. Partitions

A partition of a finite set B is a collection of subsets, called parts, which are pairwise disjoint and whose union is the whole of B. We denote the parts of a partition f as $P_i(f)$. If every part of f is contained in a unique part of g, we say f refines g. The equality partition E_B with $|B|$ parts refines any other partition, while the universal partition (with only one part) is refined by any other partition of B. The common refinement of two partitions f, g of B is given by $h := f \vee g$ with parts:

$$P_{i,j}(h) = P_i(f) \cap P_j(g) : P_i(f) \cap P_j(g) \neq \emptyset.$$

We shall usually consider a tuple of n partitions $f = (f_1, \ldots, f_n)$ of the same set assigned to elements of a finite set V with n elements. In that case, for any $X \subseteq V$, we denote the common refinement of all $f_v, v \in X$ as $f_X := \bigvee_{v \in X} f_v$. For any $X, Y \subseteq V$, we then have $f_{X \cup Y} = f_X \vee f_Y$.

2.3. Closure Solvability and Entropy

We now review the closure solvability problem [8]. The instance of the problem consists of a closure operator cl on V with rank r and a finite set A with $|A| \geq 2$, referred to as the alphabet.

Definition 1. *A coding function for cl over A is a family f of n partitions of A^r (the set of strings of length r over A) into at most $|A|$ parts, such that $f_X = f_{\mathrm{cl}(X)}$ for all $X \subseteq V$.*

We remark that the family of partitions $f = (f_1, \ldots, f_n)$ where f_i is the partition of A^r with only one part is a coding function for any closure operator of rank r over A.

The problem is to determine whether there exists a coding function for cl over A, such that f_V has A^r parts. That is, we want to determine whether there exists an n-tuple $f = (f_1, \ldots, f_n)$ of partitions of A^r in at most $|A|$ parts, such that:

$$f_X = f_{\mathrm{cl}(X)} \quad \text{for all } X \subseteq V,$$
$$f_V = E_{A^r}.$$

We make several remarks concerning the closure solvability problem.

(1) The solvability problem could be defined as searching for families of partitions of any set B with $|B| \geq |A|^r$, such that $f_V = E_B$. However, this can only occur if $|B| = |A|^r$; moreover, since only the cardinality of B matters, we can assume without loss that $B = A^r$.

(2) A coding function f naturally yields a closure operator cl_f on V, where $\mathrm{cl}_f(X) = \{v \in V : f_{X \cup v} = f_X\} = \bigcup \{Y : f_Y = f_X\}$; we then have $\mathrm{cl} \leq \mathrm{cl}_f$. Therefore, if cl_2 is solvable, then any cl_1 with the same rank and $\mathrm{cl}_1 \leq \mathrm{cl}_2$ is also solvable.

For any partition g of A^r, the entropy of g is defined as the traditional entropy of the probability distribution where each event is a part with probability proportional to its size, scaled by the log of the alphabet size, *i.e.*,

$$H(g) := r - |A|^{-r} \sum_i |P_i(g)| \log_{|A|} |P_i(g)|.$$

The equality partition on A^r is the only partition with full entropy r. Denoting $H_f(X) := H(f_X)$, we can recast the conditions above as:

$$H_f(v) \leq 1 \quad \text{for all } v \in V,$$
$$H_f(X) = H_f(\mathrm{cl}(X)) \quad \text{for all } X \subseteq V,$$
$$H_f(V) = r.$$

The first two conditions are equivalent to f being a coding function. In general, the rank cannot always be attained; hence, we define the entropy of a closure operator cl over A as the maximum entropy of any coding function for it:

$$H(\mathrm{cl}, A) := \max\{H_f(V) : f \text{ coding function for } \mathrm{cl} \text{ over } A\}.$$

The entropy of cl is defined to be the supremum of all $H(\mathrm{cl}, A)$.

2.4. Guessing Game and Closure Solvability

The guessing game was first proposed for the study of network coding solvability by Riis. It is a cooperative game with n players, where each can only see a number of hats of the other players, but not their own. All of the players must guess the color of their own hat at the same time; the team wins if everyone guesses correctly. The aim of the guessing game is to devise a guessing strategy (a protocol), which maximises the number of winning configurations.

More formally, a configuration on a digraph D on V over a finite alphabet A is simply an n-tuple $x = (x_1, \ldots, x_n) \in A^n$. A protocol $f = (f_1, \ldots, f_n)$ of D is a mapping $f : A^n \to A^n$, such that $f(x)$ is locally defined, *i.e.*, $f_v(x) = f_v(x_{v^-})$ for all v. The fixed configurations of f are all of the configurations $x \in A^n$, such that $f(x) = x$: $\mathrm{Fix}(f) = \{x \in A^n : f(x) = x\}$. The guessing number of D is then defined as the logarithm of the maximum number of configurations fixed by a protocol of D:

$$g(D, A) = \max_f \left\{ \log_{|A|} |\mathrm{Fix}(f)| \right\}.$$

The guessing game on D is equivalent to the solvability problem for cl_D [8].

3. Rank Functions of Closure Operators

In this section, we investigate the properties of closure operators in general and we derive bounds on the entropy of their coding functions. We shall introduce four kinds of ranks for any closure operator. It is worth noting that they are all distinct from the so-called rank function of a closure operator studied in [20].

3.1. Inner and Outer Ranks

First of all, we are interested in upper bounds on the entropy of coding functions.

Definition 2. *The inner rank and outer rank of a subset X of vertices are respectively given by:*

$$\mathrm{ir}(X) := \min\{|b| : \mathrm{cl}(X) = \mathrm{cl}(b)\}$$
$$\mathrm{or}(X) := \min\{|b| : X \subseteq \mathrm{cl}(b)\} = \min\{|b| : \mathrm{cl}(X) \subseteq \mathrm{cl}(b)\}.$$

Although the notations should reflect which closure operator is used in order to be rigorous, we shall usually omit this dependence for the sake of clarity. Instead, if the closure operator is "decorated" by subscripts or superscripts, then the corresponding parameters will be decorated in the same fashion.

A set i with $|i| = \mathrm{ir}(X)$ and $\mathrm{cl}(i) = \mathrm{cl}(X)$ is called an inner basis of X; similarly a set o with $|o| = \mathrm{or}(X)$ and $\mathrm{cl}(X) \subseteq \mathrm{cl}(o)$ is called an outer basis of X.

The following properties are an easy exercise.

Proposition 1. *For any $X, Y \subseteq V$,*

(1) $\mathrm{or}(\mathrm{cl}(X)) = \mathrm{or}(X)$ *and* $\mathrm{ir}(\mathrm{cl}(X)) = \mathrm{ir}(X)$;

(2) $\mathrm{or}(X) \leq \mathrm{ir}(X) \leq |X|$;

(3) $\mathrm{or}(X \cup Y) \leq \mathrm{or}(X) + \mathrm{or}(Y)$ *and* $\mathrm{ir}(X \cup Y) \leq \mathrm{ir}(X) + \mathrm{ir}(Y)$;

(4) $\mathrm{or}(\emptyset) = \mathrm{ir}(\emptyset) = 0$ *and* $\mathrm{or}(V) = \mathrm{ir}(V) = r$;

(5) if $X \subseteq Y$, *then* $\mathrm{or}(X) \leq \mathrm{or}(Y)$.

The closure of the empty set is the only closed set of (inner and outer) rank zero, while V is not necessarily the unique closed set of (inner or outer) rank r.

Note that the inner rank is not monotonic, as seen in the example in Figure 1. We have $\mathrm{cl}_D(4) = V$ and, hence, $\mathrm{ir}_D(V) = 1$, while $\mathrm{ir}_D(123) = 2$ for $\mathrm{cl}_D(12) = 123$, while $\mathrm{cl}_D(v) = v$ for any $v \in 123$.

Figure 1. Example where the inner rank is not monotonic.
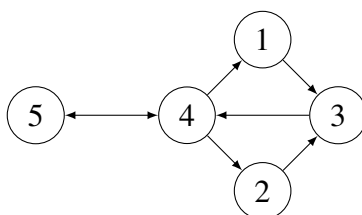
If $\mathrm{cl}_1(X) \subseteq \mathrm{cl}_2(X)$ for some X, then $\mathrm{or}_1(X) \geq \mathrm{or}_2(X)$. Indeed, any outer basis of X with respect to cl_1 is also an outer basis of X with respect to cl_2. In particular, if $\mathrm{cl}_1 \leq \mathrm{cl}_2$, then $\mathrm{or}_1(X) \geq \mathrm{or}_2(X)$ for all X.

Lemma 1. *Let $G : 2^V \to \mathbb{R}$ satisfying $0 \leq G(X) \leq |X|$ and $G(\mathrm{cl}(X)) = G(X)$ for all $X \subseteq V$. Then, $G(X) \leq \mathrm{ir}(X)$ for all X. Furthermore, if $X \subseteq Y$ implies $G(X) \leq G(Y)$, then $G(X) \leq \mathrm{or}(X)$ for all X.*

Proof. First, if i is an inner basis of X, then $G(X) = G(\mathrm{cl}(i)) = G(i) \leq |i| = \mathrm{ir}(X)$. Second, if o is an outer basis of X, $G(X) \leq G(\mathrm{cl}(o)) = G(o) \leq |o| = \mathrm{or}(X)$. $\square$

This Lemma proves that we get subadditivity for free. Since the entropy satisfies all of the conditions of Lemma 1, we obtain an upper bound on the entropy.

Corollary 1. *For any coding function f and any $X \subseteq V$, $H_f(X) \leq \mathrm{or}(X)$.*

3.2. Flats and Span

Before we move on to lower bounds on the entropy, we define two fundamental concepts.

Definition 3. *A flat is a subset F of vertices for which there is no $X \supset F$ with $\mathrm{or}(X) = \mathrm{or}(F)$.*

Proposition 2. *Flats satisfy the following properties.*

(1) $\mathrm{cl}(\emptyset)$ is the only flat with rank zero, and V is the only flat with rank r.

(2) any flat F is a closed set;

(3) $\mathrm{or}(F) = \mathrm{ir}(F)$;

(4) for any X, there exists a flat $F \supseteq X$ with $\mathrm{or}(F) = \mathrm{or}(X)$.

Proof. (1) is trivial.

(2) Since $\mathrm{cl}(F)$ contains F while having the same rank as F, it cannot properly contain F.

(3) Let o be an outer basis of F. Since $F \subseteq \mathrm{cl}(o)$ while $\mathrm{or}(F) = \mathrm{or}(\mathrm{cl}(o))$, we obtain $F = \mathrm{cl}(o)$ and o is an inner basis of F.

(4) For any X, let C be a set with rank $\mathrm{or}(X)$ and containing X of largest cardinality, then there exists no G, such that $C \subset G$ and $\mathrm{or}(G) = \mathrm{or}(X) = \mathrm{or}(C)$. $\square$

It is worth noting that there are closed sets that are not flats. For example, consider the following closure operator on $V = \{1, \ldots, n\}$, where $\mathrm{cl}(X) = \{1, \ldots, \max(X)\}$. Then, it has rank one and, hence, only two flats (the empty set and V), while it has $n + 1$ closed sets (the empty set and $\mathrm{cl}(i)$ for all i). We shall clarify the relationship between closed sets and flats below.

Definition 4. *For any $X \subseteq V$, the union of all flats containing X with outer rank equal to that of X is referred to as the span of X, i.e.,*

$$\mathrm{span}(X) := \bigcup \{F : F \text{ flat}, X \subseteq F, \mathrm{or}(F) = \mathrm{or}(X)\}.$$

Proposition 3. *For any X,*

(1) $\mathrm{cl}(X) \subseteq \mathrm{span}(X)$ *with equality if and only if* $\mathrm{cl}(X)$ *is a flat;*

(2) $\mathrm{span}(\mathrm{cl}(X)) = \mathrm{span}(X)$*;*

(3) $\mathrm{span}(X) := \{v \in V : \mathrm{or}(X \cup v) = \mathrm{or}(X)\}$*.*

Proof. The first two properties follow directly from the definition. Suppose $v \in F$, a flat containing X with $\mathrm{or}(F) = \mathrm{or}(X)$, then $\mathrm{or}(X \cup v) \le \mathrm{or}(F) = \mathrm{or}(X)$. Conversely, if $\mathrm{or}(X \cup w) = \mathrm{or}(X)$, then $X \cup w$ is contained in a flat with the same outer rank as X and, hence, in $\mathrm{span}(X)$. $\square$

Flats and spans provide two alternate axioms for matroids.

Theorem 1. *The following are equivalent:*

(1) cl *is a matroid;*

(2) *all closed sets are flats, i.e.,* $\mathrm{cl}(X) = \mathrm{span}(X)$ *for all* $X \subseteq V$*;*

(3) *all closed sets are spans, i.e., for all* $X \subseteq V$*, there exists* $Y \subseteq V$*, such that* $\mathrm{cl}(X) = \mathrm{span}(Y)$*.*

Proof. The first property clearly implies the third one. Let us now prove that the second property implies the first one. Let $X \subseteq V$, $v \in V$ and $u \in \mathrm{cl}(X \cup v) \backslash \mathrm{cl}(X)$, then $\mathrm{or}(X \cup u) = \mathrm{or}(X) + 1 = \mathrm{or}(X \cup v)$ and, hence, $\mathrm{cl}(X \cup u) = \mathrm{cl}(X \cup v)$. Thus, cl satisfies the Steinitz–Mac Lane exchange axiom.

We now prove that the third property implies the second. Suppose all closed sets are spans, then we shall prove that all closed sets of outer rank k are flats, by induction on $0 \le k \le r$. This is clear for $k = 0$; hence, suppose it holds for up to $k - 1$. Consider a minimal closed set c of outer rank k, *i.e.*, $\mathrm{or}(c) = k$ and $\mathrm{or}(c') = k - 1$ for any closed set $c' \subset c$. By hypothesis, we have $c = \mathrm{span}(Y)$ for some $Y \subseteq c$; we now prove that $c = \mathrm{cl}(Y)$. Suppose that $\mathrm{cl}(Y) \subset c$, then $\mathrm{cl}(Y) = c'$, a closet set of outer rank at most $k - 1$. Then, c' is a flat, *i.e.*, $c' = \mathrm{span}(c') = \mathrm{span}(\mathrm{cl}(Y)) = \mathrm{span}(Y) = c$, a contradiction. Thus, $c = \mathrm{span}(c)$ and c is a flat. $\square$

There are solvable closure operators that are not matroids, e.g., the undirected graph $\bar{C}_4$ displayed in Figure 2. It is solvable because it has rank two and contains $K_2 \cup K_2$. More explicitly, the following is a solution for it over any alphabet:

$$\begin{aligned}
P_i(y) :=& \{x \in A^2 : x_i = y\}, \quad i \in \{1, 2\} \\
f_1 = f_3 =& \{P_1(y) : y \in A\} \\
f_2 = f_4 =& \{P_2(y) : y \in A\}
\end{aligned}$$

In that case, note that the outer rank is submodular, and hence, $\mathrm{span}_{\bar{C}_4} = U_{2,4}$ is a matroid; however, $\mathrm{cl}_{\bar{C}_4}$ is not a matroid itself.

We would like to explain the significance of flats in matroids for random network coding. A model for noncoherent random network coding based on matroids is proposed in [21], which generalises routing (a special case for the uniform matroid), linear network coding (the projective geometry) and affine network coding (the affine geometry). In order to combine the messages they receive, the intermediate nodes

select a random element from the closure of the received messages. The model is based on matroids, because all closed sets are flats, hence a new message is either in the closure of all of the previously received messages (and is not informative) or it increases the outer rank (and is fully informative).

Figure 2. The graph $\bar{C}_4$ whose closure operator is solvable, but not a matroid.
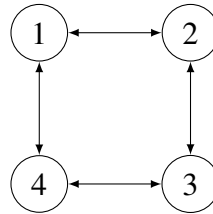
3.3. Upper and Lower Ranks

We are now interested in lower bounds on the entropy of coding functions. Since any closure operator has a trivial coding function with entropy zero (where the universal partition is placed on every vertex), the entropy of any coding function cannot be bounded below. Therefore, most of our bounds will apply to solutions only.

Definition 5. *The lower rank and upper rank of X are respectively defined as:*

$$\mathrm{lr}(X) := \min\{|Y| : \mathrm{cl}(Y \cup (V \backslash X)) = V\},$$
$$\mathrm{ur}(X) := r - \mathrm{lr}(V \backslash X).$$

A few elementary properties of the lower and upper ranks are listed below. Again, if $\mathrm{cl}_1 \leq \mathrm{cl}_2$, then $\mathrm{lr}_1(X) \geq \mathrm{lr}_2(X)$ and $\mathrm{ur}_1(X) \geq \mathrm{ur}_2(X)$ for all $X \subseteq V$.

Lemma 2. *The following hold:*

(1) $\mathrm{lr}(V) = \mathrm{ur}(V) = r$ *and* $\mathrm{lr}(\emptyset) = \mathrm{ur}(\emptyset) = 0$.

(2) *For any $X \subseteq V$, $\mathrm{lr}(X) = 0$ if and only if $\mathrm{cl}(V \backslash X) = V$. Hence, $\mathrm{ur}(X) = r$ if and only if* $\mathrm{cl}(X) = V$.

(3) *For any $X \subseteq V$,*

$$\mathrm{ur}(X) = r - \min\{\mathrm{or}(Y) : \mathrm{cl}(X \cup Y) = V\}$$
$$= r - \min\{\mathrm{or}(F) : F \text{ flat and } \mathrm{cl}(X \cup F) = V\}.$$

(4) *If $X \subseteq Z$, then $\mathrm{ur}(X) \leq \mathrm{ur}(Z)$ and $\mathrm{lr}(X) \leq \mathrm{lr}(Z)$.*

(5) $\mathrm{ur}(X) = \mathrm{ur}(\mathrm{cl}(X))$.

(6) $\mathrm{lr}(X) \leq \mathrm{ur}(X) \leq \mathrm{or}(X)$.

Proof. The first three properties are easily proven. Property (4) for the upper rank follows from Property (3); the result for the lower rank follows from $\text{lr}(X) = r - \text{ur}(V \backslash X)$. For Property (5), Property (4) yields $\text{ur}(X) \leq \text{ur}(\text{cl}(X))$, while $\text{cl}(X \cup Y) = \text{cl}(\text{cl}(X) \cup Y)$ yields the reverse inequality. We now prove Property (6). The inequality $\text{ur}(X) \leq \text{or}(X)$ follows from the subadditivity of the outer rank. To prove that $\text{lr}(X) \leq \text{ur}(X)$, let b be a basis for cl. Then:

$$V = \text{cl}(b) = \text{cl}\left\{(b \cap X) \cup (b \cap (V \backslash X))\right\} \subseteq \text{cl}\left\{(b \cap X) \cup (V \backslash X)\right\},$$

and hence, $\text{cl}\left\{(b \cap X) \cup (V \backslash X)\right\} = V$, thus $|b \cap X| \geq \text{lr}(X)$. Similarly, $|b \cap (V \backslash X)| \geq \text{lr}(V \backslash X)$, and hence, $r = |b| \geq \text{lr}(X) + \text{lr}(V \backslash X)$. $\square$

We remark that for any solution f, we have $r = H_f(V) \leq \text{or}(X) + \text{or}(Y)$ for any X, Y, such that $\text{cl}(X \cup Y) = V$. Therefore, we obtain:

$$H_f(X) \geq \text{ur}(X)$$

for all $X \subseteq V$.

Corollary 2. *For any solution f of cl and any $X \subseteq V$,*

$$r - H_f(V \backslash \text{cl}(X)) \leq \text{lr}(\text{cl}(X)) \leq \text{ur}(X) \leq H_f(X) \leq \text{or}(X).$$

Note that a trivial lower bound on $H_f(X)$ (where f is a solution) is given by $r - H_f(V \backslash X)$. Therefore, the intermediate bounds on $H_f(X)$ in Corollary 2 refine this trivial bound.

Some of the results above can be generalised for any coding function f: denoting:

$$\text{lr}_f(X) = \min\{H_f(Y) : \text{cl}(Y \cup (V \backslash X)) = V\},$$
$$\text{ur}_f(X) = H_f(V) - \text{lr}_f(V \backslash X),$$

we obtain:

$$H_f(V) - H_f(V \backslash \text{cl}(X)) \leq \text{lr}_f(\text{cl}(X)) \leq \text{ur}_f(X) \leq H_f(X) \leq \text{or}(X).$$

We finish this subsection by remarking that Theorem 1 has an analogue for the upper rank. Namely, define an upper flat as a set F, such that $F \subset X$ implies $\text{ur}(X) > \text{ur}(F)$; define also the upper span of X as:

$$\text{uspan}(X) := \bigcup\{F : F \text{ upper flat}, X \subseteq F, \text{ur}(F) = \text{ur}(X)\} = \{v \in V : \text{ur}(X \cup v) = \text{ur}(X)\}.$$

Theorem 2. *The following are equivalent:*

(1) cl *is a matroid;*

(2) *all closed sets are upper flats, i.e.,* $\text{cl}(X) = \text{uspan}(X)$ *for all* $X \subseteq V$;

(3) *all closed sets are upper spans, i.e., for all* $X \subseteq V$, *there exists* $Y \subseteq V$, *such that* $\text{cl}(X) = \text{uspan}(Y)$.

3.4. Inner and Outer Complemented Sets

We are now interested in a case where the bounds on the entropy are tight.

Definition 6. *We say a set X is outer complemented if* $\mathrm{or}(X) = \mathrm{ur}(X)$. *Moreover, we say it is inner complemented if* $\mathrm{ir}(X) = \mathrm{ur}(X)$.

Therefore, if X is outer complemented, then $H_f(X) = \mathrm{or}(X) = \mathrm{ur}(X)$ for any solution f.

Remark that X is outer (inner) complemented if and only if $\mathrm{cl}(X)$ is outer (inner) complemented.

Proposition 4. *The following are equivalent:*

(1) X is outer complemented;

(2) there exists Z, such that $\mathrm{or}(X) + \mathrm{or}(Z) = r$, $\mathrm{cl}(X \cup Z) = V$ and $X \cap Z = \emptyset$;

(3) any outer basis of X is contained in a basis of V.

Similar results hold for inner complemented sets. The following are equivalent:

(1) X is inner complemented;

(2) X is outer complemented and $\mathrm{ir}(X) = \mathrm{or}(X)$;

(3) any inner basis of X is contained in a basis of V.

Proof. The equivalence of the first two properties is easily shown. If X is outer complemented, let o be an outer basis of X, and let Z satisfy $\mathrm{cl}(X \cup Z) = V$ and $|Z| = r - \mathrm{or}(X)$. Then, $o \cup Z$ is a basis of V. Conversely, if any outer basis can be extended to a basis, then any such extension is a valid Z for Property (2). The properties for an inner complemented set are easy to prove. □

We saw earlier that $\mathrm{cl}(X) \subseteq \mathrm{cl}_f(X)$ for any coding function f and any X. This can be refined when f is a solution and X is outer complemented.

Lemma 3. *If f is a solution of* cl, *then* $\mathrm{cl}(\mathrm{span}(X)) \subseteq \mathrm{cl}_f(X)$ *for any outer complemented X.*

Proof. For any outer complemented X, we have $H_f(X) = \mathrm{or}(X)$. Suppose $v \in \mathrm{span}(X)$, then $\mathrm{or}(X) = \mathrm{or}(X \cup v) \geq H_f(X \cup v) \geq H_f(X) = \mathrm{or}(X)$ and, hence, $v \in \mathrm{cl}_f(X)$. Since $\mathrm{cl}_f(X)$ is a closed set of cl, we easily obtain that $\mathrm{cl}(\mathrm{span}(X)) \subseteq \mathrm{cl}_f(X)$. □

Corollary 3. *If there exists an outer complemented set X, such that its span has higher outer rank and is also outer complemented, then* cl *is not solvable over any alphabet.*

By extension, we say that cl is outer complemented if all sets are outer complemented. We can characterise the solvable outer complemented closure operators.

Theorem 3. *Suppose that* cl *has rank r and is outer complemented. Then,* cl *is solvable if and only if* span *is a solvable matroid with rank r.*

Proof. If all sets are outer complemented, then any solution f of cl is also a coding function of span, since $\mathrm{span}(X) = \{v \in V : H_f(X \cup v) = H_f(X)\}$. Since the outer rank is equal to the entropy H_f, it is submodular, and hence, span is a matroid whose rank function is given by the outer rank. Thus, span has rank r and f is a solution for it. Conversely, if span is a solvable matroid with rank r, then we have $\mathrm{cl} \leq \mathrm{span}$ and cl is solvable. $\square$

For instance, for the undirected cycle $\bar{C}_5$ in Figure 3, $\mathrm{cl}_{\bar{C}_5}$ is outer complemented, though the outer rank is not submodular; hence, span is not a matroid. As such, $\bar{C}_5$ is not solvable (its entropy is actually 2.5 [10]).

Figure 3. The graph $\bar{C}_5$ whose closure operator is outer complemented and not solvable.
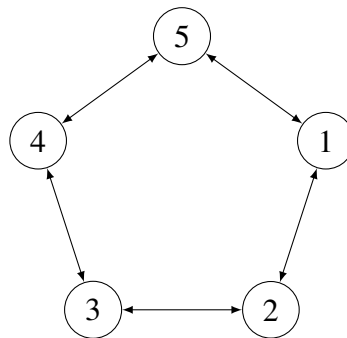
We would like to emphasize that if all sets are outer complemented, then the outer rank must be submodular, *i.e.*, the rank function of a matroid. However, this does not imply that cl should be a matroid itself. For instance, consider cl defined on $\{1, 2, 3\}$ as follows: $\mathrm{cl}(1) = 12$, $\mathrm{cl}(2) = 2$, $\mathrm{cl}(3) = 3$, $\mathrm{cl}(13) = \mathrm{cl}(23) = 123$. Then, any set is inner complemented, cl is solvable (by letting $f_1 = f_2$ and f_3, such that $f_1 \vee f_3 = E_{A^2}$), but cl is not a matroid.

3.5. Combining Closure Operators

In this subsection, V_1 and V_2 are disjoint sets of respective cardinalities n_1 and n_2; cl_1 and cl_2 are closure operators on V_1 with rank r_1 and on V_2 with rank r_2, respectively. We further let $V = V_1 \cup V_2$ and for any $X \subseteq V$; we shall denote $X_1 = X \cap V_1$ and $X_2 \cap V_2$. Different ways of combining closure operators have been proposed in [8].

Definition 7. *The disjoint, unidirectional and bidirectional unions of cl_1 and cl_2 are, respectively:*

$$\mathrm{cl}_1 \cup \mathrm{cl}_2(X) := \mathrm{cl}_1(X_1) \cup \mathrm{cl}_2(X_2)$$

$$\mathrm{cl}_1\vec{\cup}\mathrm{cl}_2(X) := \begin{cases} V_1 \cup \mathrm{cl}_2(X_2) & \textit{if } \mathrm{cl}_1(X_1) = V_1 \\ \mathrm{cl}_1(X_1) \cup X_2 & \textit{otherwise} \end{cases}$$

$$\mathrm{cl}_1\bar{\cup}\mathrm{cl}_2(X) := \begin{cases} V_1 \cup \mathrm{cl}_2(X_2) & \textit{if } X_1 = V_1 \\ V_2 \cup \mathrm{cl}_2(X_1) & \textit{if } X_2 = V_2 \\ X & \textit{otherwise}. \end{cases}$$

If cl is a closure operator on V satisfying $\mathrm{cl}_1 \vec{\cup} \mathrm{cl}_2 \leq \mathrm{cl} \leq \mathrm{cl}_1 \cup \mathrm{cl}_2$, it has rank $r_1 + r_2$ and entropy $H(\mathrm{cl}_1) + H(\mathrm{cl}_2)$. We can then split the problems into two parts. In that case, we also have:

$$\mathrm{cl}_1(X_1) = \mathrm{cl}(X) \cap V_1 = \mathrm{cl}(X_1 \cup V_2) \cap V_1 = \mathrm{cl}(X_1) \cap V_1$$

for all $X \subseteq V$, *i.e.*, V_2 has no influence on $\mathrm{cl}(X)$ on V_1.

The rank of the bidirectional union is given by:

$$r(\mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2) = \min\{n_1 + r_2, n_2 + r_1\},$$

while its entropy only satisfies the inequality:

$$H(\mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2) \leq \min\{n_1 + H(\mathrm{cl}_2), n_2 + H(\mathrm{cl}_1)\}.$$

We can determine how the four rank functions given above behave with regards to the three types of union.

Proposition 5. *For the disjoint union, let* $\mathrm{cl}_\cup := \mathrm{cl}_1 \cup \mathrm{cl}_2$, *then:*

$$r_\cup = r_1 + r_2$$
$$\mathrm{or}_\cup(X) = \mathrm{or}_1(X_1) + \mathrm{or}_2(X_2)$$
$$\mathrm{ir}_\cup(X) = \mathrm{ir}_1(X_1) + \mathrm{ir}_2(X_2)$$
$$\mathrm{ur}_\cup(X) = \mathrm{ur}_1(X_1) + \mathrm{ur}_2(X_2)$$
$$\mathrm{lr}_\cup(X) = \mathrm{lr}_1(X_1) + \mathrm{lr}_2(X_2).$$

For the unidirectional union, let $\mathrm{cl}_{\vec{\cup}} := \mathrm{cl}_1 \vec{\cup} \mathrm{cl}_2$, *then:*

$$r_{\vec{\cup}} = r_1 + r_2$$
$$\mathrm{or}_{\vec{\cup}}(X) = \min\{r_1 + \mathrm{or}_2(X_2), \mathrm{or}_1(X_1) + |X_2|\}$$
$$\mathrm{ir}_{\vec{\cup}}(X) = \min\{r_1 + \mathrm{ir}_2(X_2), \mathrm{ir}_1(X_1) + |X_2|\}$$
$$\mathrm{ur}_{\vec{\cup}}(X) = \mathrm{ur}_1(X_1) + \mathrm{ur}_2(X_2)$$
$$\mathrm{lr}_{\vec{\cup}}(X) = \mathrm{lr}_1(X_1) + \mathrm{lr}_2(X_2).$$

For the bidirectional union, let $\mathrm{cl}_{\bar{\cup}} := \mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2$, *then:*

$$r_{\bar{\cup}} = \min\{n_1 + r_2, n_2 + r_1\}$$
$$\mathrm{or}_{\bar{\cup}}(X) = \min\{n_1 + \mathrm{or}_2(X_2), n_2 + \mathrm{or}_1(X_1), |X|\}$$
$$\mathrm{ir}_{\bar{\cup}}(X) = \begin{cases} \min\{n_1 + r_2, n_2 + r_1\} & \textit{if } \mathrm{cl}(X) = V \\ n_1 + \mathrm{ir}_2(X_2) & \textit{if } X_1 = V_1, \mathrm{cl}_2(X_2) \neq V_2 \\ n_2 + \mathrm{ir}_1(X_1) & \textit{if } X_2 = V_2, \mathrm{cl}_1(X_1) \neq V_1 \\ |X| & \textit{otherwise} \end{cases}$$
$$\mathrm{ur}_{\bar{\cup}}(X) = r_{\bar{\cup}} - \min\{n_1 - |X_1| + r_2 - \mathrm{ur}_2(X_2), n_2 - |X_2| + r_1 - \mathrm{ur}_1(X_1)\}$$
$$\mathrm{lr}_{\bar{\cup}}(X) = \min\{|X_1| + \mathrm{lr}_2(X_2), |X_2| + \mathrm{lr}_1(X_1)\}.$$

Proof. The results for the disjoint union easily follow from the definitions. We then turn to the unidirectional union. Again, we remark that $\mathrm{cl}_{\cup}(X) = V$ if and only if $\mathrm{cl}_1(X_1) = V_1$ and $\mathrm{cl}_2(X_2) = V_2$; this gives the rank, the upper rank of X and then its lower rank. For the upper rank, we have $X \subseteq \mathrm{cl}_{\cup}(o)$ if and only if either $\mathrm{cl}_1(o_1) = V_1, X_2 \subseteq \mathrm{cl}_2(o_2)$ or $X_1 \subseteq \mathrm{cl}_1(o_1), X_2 \subseteq o_2$. The proof for the inner rank is similar.

For the bidirectional union, we have $X \subseteq \mathrm{cl}_{\cup}(o)$ if and only if $o_1 = V_1, X_2 \subseteq \mathrm{cl}_2(o_2)$ or $o_2 = V_2, X_1 \subseteq \mathrm{cl}_1(o_1)$ or $X \subseteq o$; this yields the outer rank. The inner rank is obtained by considering each case separately. If $X = V$, then $\mathrm{cl}_{\cup}(i) = \mathrm{cl}_{\cup}(X) = V$ if and only if $i_1 = V_1, \mathrm{cl}_2(i_2) = V_2$ or $i_2 = V_2, \mathrm{cl}_1(i_1) = V_1$. If $X_1 = V_1$, but $\mathrm{cl}_2(X_2) \neq V_2$, then $\mathrm{cl}_{\cup}(i) = \mathrm{cl}_{\cup}(X)$ if and only if $i_1 = V_1, \mathrm{cl}_2(i_2) = \mathrm{cl}_2(X_2)$. The third case comes from symmetry. Finally, if $X_1 \neq V_1$ and $X_2 \neq V_2$, then $\mathrm{cl}_{\cup}(i) = \mathrm{cl}_{\cup}(X) = X$ if and only if $i = X$. For the upper rank, we remark that $\mathrm{cl}_{\cup}(X \cup Y) = V$ if and only if either $X_1 \cup Y_1 = V_1, \mathrm{cl}_2(X_2 \cup Y_2) = V_2$ or $X_2 \cup Y_2 = V_2, \mathrm{cl}_1(X_1 \cup Y_1) = V_1$. The lower rank follows from the upper rank. $\square$

4. Shannon Entropy

Since finding the entropy of a digraph is difficult in general, [9,10] developed the idea of Shannon entropy of a graph. The main idea is to maximise over all functions that satisfy some of the properties of an entropic function, notably submodularity. This idea can be adapted to general closure operators. For any closure operator cl on V, a Shannon function for cl can be viewed as a cl-compatible polymatroid.

Definition 8. *For any closure operator* cl *on* V, *a Shannon function for* cl *is a function* $r : 2^V \to \mathbb{R}$, *such that:*

(1) if $X \subseteq V$, *then*

$$0 \leq r(X) \leq |X|,$$

(2) r *is increasing, i.e., if* $X \subseteq Y \subseteq V$, *then*

$$r(X) \leq r(Y),$$

(3) r *is submodular, i.e., if* $X, Y \subseteq V$, *then:*

$$r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y),$$

(4) for all $X \subseteq V$,

$$r(X) = r(\mathrm{cl}(X)).$$

The maximum value of $r(V)$ *over all Shannon functions for* cl *is called the Shannon entropy of* cl *and is denoted by* $\mathrm{SE}(\mathrm{cl})$.

Any Shannon function also satisfies the conditions of Lemma 1, hence $\mathrm{SE}(\mathrm{cl}) \leq \mathrm{or}(V) = r$. Moreover, it is clear that if $\mathrm{cl}_1 \leq \mathrm{cl}_2$, then $\mathrm{SE}(\mathrm{cl}_1) \geq \mathrm{SE}(\mathrm{cl}_2)$.

4.1. Shannon Entropy and Combining Closure Operators

Lemma 4. *If* $\mathrm{cl}_1 \vec{\mathbb{U}} \mathrm{cl}_2 \leq \mathrm{cl} \leq \mathrm{cl}_1 \cup \mathrm{cl}_2$, *then for any Shannon function* r *for* cl, *the function:*

$$r'(X) := r(X \cap V_1) + r(X \cup V_1) - r(V_1)$$

is a Shannon function for cl, *such that* $r'(X) = r'(X_1) + r'(X_2)$ *and* $r'(V) = r(V)$.

Proof. Only the closure property is nontrivial to verify. Since $\mathrm{cl}(X) \cap V_1 = \mathrm{cl}(X_1) \cap V_1$, we obtain:

$$r'(\mathrm{cl}(X)) = r(\mathrm{cl}(X) \cap V_1) + r(\mathrm{cl}(X) \cup V_1) - r(V_1) \leq r(\mathrm{cl}(X_1)) + r(\mathrm{cl}(X \cup V_1)) - r(V_1) = r'(X).$$

□

Proposition 6. *If* $\mathrm{cl}_1 \vec{\mathbb{U}} \mathrm{cl}_2 \leq \mathrm{cl} \leq \mathrm{cl}_1 \cup \mathrm{cl}_2$, *then:*

$$\mathrm{SE}(\mathrm{cl}) = \mathrm{SE}(\mathrm{cl}_1) + \mathrm{SE}(\mathrm{cl}_2).$$

Proof. First of all, it is clear that $\mathrm{SE}(\mathrm{cl}) \geq \mathrm{SE}(\mathrm{cl}_1) + \mathrm{SE}(\mathrm{cl}_2)$. Indeed, let r_i be a Shannon function for cl_i, then r defined by $r(X) := r_1(X_1) + r_2(X_2)$ is a Shannon function for $\mathrm{cl}_1 \cup \mathrm{cl}_2$.

We now show the reverse inequality. By Lemma 4, there exists a Shannon function r for cl with $r(X) = r(X_1) + r(X_2)$ and $r(V) = \mathrm{SE}(\mathrm{cl})$. It is easily seen that the restriction $r_2(X)$ of $r(X)$ to V_2 is a Shannon function for cl_2, hence $r_2(V_2) = r(V_2) \leq \mathrm{SE}(\mathrm{cl}_2)$. Furthermore, define the function $r_1 : 2^{V_1} \to \mathbb{R}$ as:

$$r_1(X) := r(X \cup V_2) - r(V_2).$$

We check that r_1 is indeed a Shannon function for cl_1. The first two properties are straightforward, while submodularity comes from:

$$
\begin{aligned}
r_1(X) + r_1(Y) &= r(X \cup V_2) + r(Y \cup V_2) - 2r(V_2) \\
&\geq r((X \cup Y) \cup V_2) + r((X \cap Y) \cup V_2) - 2r(V_2) \\
&= r_1(X \cup Y) + r_1(X \cap Y)
\end{aligned}
$$

and the closure property comes from the fact that $\mathrm{cl}_1(X) = \mathrm{cl}(X \cup V_2) \backslash V_2$.

$$r_1(\mathrm{cl}_1(X)) = r(\mathrm{cl}_1(X) \cup V_2) - r(V_2) = r(\mathrm{cl}(X \cup V_2)) - r(V_2) = r(X \cup V_2) - r(V_2) = r_1(X).$$

Thus,

$$r(V) = r_1(V_1) + r_2(V_2) \leq \mathrm{SE}(\mathrm{cl}_1) + \mathrm{SE}(\mathrm{cl}_2).$$

□

The Shannon entropy of the bidirectional union satisfies a similar inequality to the one for the corresponding entropy.

Proposition 7. *For any* cl_1 *and* cl_2, *we have:*

$$\mathrm{SE}(\mathrm{cl}_1 \vec{\mathbb{U}} \mathrm{cl}_2) \leq \min\{\mathrm{SE}(\mathrm{cl}_1) + n_2, \mathrm{SE}(\mathrm{cl}_2) + n_1\}.$$

Proof. We say a function $r : 2^V \to 2^V$ is a V_1-function if it satisfies all of the properties of a Shannon function, but only for all X, Y containing V_1. The maximum value of $r(V)$ over any V_1-function, denoted as S, is greater than or equal to $\mathrm{SE}(\mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2)$. Let r be a V_1-function and consider:

$$r_2(X) := r(X \cup V_1) - r(V_1)$$

for all $X \subseteq V_2$. We then prove that r_2 is a Shannon function for cl_2. Only Property (4) is nontrivial to check; we have:

$$r_2(\mathrm{cl}_2(X)) = r(\mathrm{cl}_2(X) \cup V_1) - r(V_1) = r(\mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2(X \cup V_1)) - r(V_1) = r(X \cup V_1) - r(V_1) = r_2(X).$$

If r achieves $r(V) = S$, we obtain $S \leq r_2(V_2) + r(V_1) \leq \mathrm{SE}(\mathrm{cl}_2) + n_1$. Thus, $\mathrm{SE}(\mathrm{cl}_1 \bar{\cup} \mathrm{cl}_2) \leq S \leq \mathrm{SE}(\mathrm{cl}_2) + n_1$. Symmetry finishes the proof. $\square$

4.2. Density of Closure Entropies

We remark that any closure operator of rank at least one has entropy at least one (assign the universal partition to every vertex in $\mathrm{cl}(\emptyset)$ and the same partition g of A^r into $|A|$ parts to any other vertices). Moreover, any D-closure for a digraph D with rank (*i.e.*, minimum feedback vertex set size) of two has entropy two; in fact, such closure operators are solvable over any sufficient large alphabet [8]. This shows that multiple unicast instances with two source-destination pairs are solvable over all sufficiently large alphabets. This proof technique cannot be generalised for general digraphs, for $\bar{C}_5$ has rank three, but entropy of only 2.5. Another direction could then be to consider other families of closure operators and find "gaps" in the entropy distribution; in particular, we may ask whether all closure operators of rank two are solvable. Theorem 4 gives an emphatic negative answer to the last question: the set of all possible closure entropies is always dense above one.

Theorem 4. *For any $r \geq 2$ and any rational number H in $(1, r]$, there exists a closure operator of rank r with entropy equal to H.*

The proof is constructive, *i.e.*, for any H, we give a closure operator with entropy equal to H and the corresponding coding functions with entropy H.

First of all, we introduce some notation regarding rooted trees. A rooted tree is a tree with a specific vertex, called the root, denoted as R. The vertices at distance k from the root form level k of the tree (hence, the root is the only vertex on level 0), this is denoted l_k. For any vertex v in level k, its parent is the only vertex adjacent to v on level $k - 1$; we denote it as $p(v)$. Moreover, we denote its ancestry as $a(v) := \{v, p(v), p^2(v), \ldots, R\}$ (remark that we include v in its ancestry). Conversely, a child of v is any vertex on level $k + 1$ adjacent to v, and any vertex without any children is a leaf of the tree. We denote the set of children of v as $c(v)$. We extend the definitions above to any set of vertices X, e.g., $p(X) = \bigcup_{v \in X} p(v)$. The following properties easily follow.

(1) If $u \in a(v)$, then $a(u) \subseteq a(v)$. Therefore, $a(a(X)) = a(X)$ for all X.

(2) If $X \subseteq Y$, then $a(X) \subseteq a(Y)$.

(3) $c(v) \subseteq a(X)$ only if $|X| \geq |c(v)|$.

Definition 9. *An (L, C)-tree, with $0 \leq L \leq C$, is a rooted tree with root R with $L + 1$ levels, such that any vertex of level k has $C - k$ children for $0 \leq k \leq L - 1$. If $L = 0$, this tree reduces to a single vertex.*

We then have:

(4) Each vertex of level $L - 1$ has $C - L + 1$ children (which are leaves).

(5) For all k, $|l_k| = \frac{C!}{(C-k)!}$.

We can express the rational number H as:

$$H = \frac{1}{D} \sum_{t=1}^{r} N_t,$$

where $D \geq \frac{r-1}{H-1}$, $0 < N_t < D$ for all $1 \leq t \leq r - 1$, and $N_r = D$. We then introduce the following closure operator. Consider r disjoint trees $T_1, \ldots, T_r$, where T_t is an $(L_t := D - N_t, C_t := DH - N_t)$ tree with root R_t for all $1 \leq t \leq r$. Then, V is the set of all vertices of the r trees and:

$$\mathrm{cl}(X) := \begin{cases} V & \text{if } \exists v : c(v) \subseteq a(X) \text{ or } X \cap T_t \neq \emptyset \, \forall 1 \leq t \leq r \\ a(X) & \text{otherwise.} \end{cases}$$

Lemma 5. *The operator* cl *is a closure operator of rank* r.

Proof. We first prove that this is indeed a closure operator. First of all, it is trivial to check that $X \subseteq \mathrm{cl}(X)$. Secondly, if $X \subseteq Y$, then we need to check that $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$. If $\mathrm{cl}(Y) = V$, this is trivial, otherwise $\mathrm{cl}(Y) = a(Y) \neq V$; and hence, $\mathrm{cl}(X) = a(X) \subseteq \mathrm{cl}(Y)$ by Proposition (2). Thirdly, we need to prove that cl is idempotent. Again, this is trivial if $\mathrm{cl}(X) = V$; hence, let $\mathrm{cl}(X) = a(X) \neq V$. By definition, there exists t, such that $X \cap T_t = \emptyset$; and hence, $a(X) \cap T_t = \emptyset$. Furthermore, for any non-leaf v, there exists a child u of v that does not belong to $a(X)$; then u does not belong to $a(a(X)) = a(X)$, either. Therefore, we have $\mathrm{cl}(a(X)) = a(a(X)) = a(X)$ by Property (1); and hence, $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(a(X)) = a(X) = \mathrm{cl}(X)$.

We now prove that it has rank r. Since the set of roots has cardinality r and intersects all trees, the rank is at most r. Conversely, suppose $\mathrm{cl}(X) = V$. Firstly, if there exists v, such that $c(V) \subseteq a(X)$, then $|X| \geq |c(v)|$ by Property (3); thus, $|X| \geq C_t - L_t + 1 = D(H - 1) + 1 \geq r$. Secondly, if X intersects all trees, then $|X| \geq r$. Thirdly, if $\mathrm{cl}(X) = a(X)$, then $a(X) = V$ and X intersects all trees; thus, $|X| \geq r$. $\square$

Lemma 6. *The entropy of* cl *is at most* H.

Proof. The proof uses the submodular inequality recursively on all levels of a tree, and then successively for all trees. More precisely, we shall use the following application of the submodular inequality: if $r : 2^V \rightarrow 2^V$ is submodular and $X_1, \ldots, X_k$ are subsets of V, such that $X_i \cap X_j = X$ for all $i \neq j$ and $\bigcup_i X_i = Y$, we have:

$$r(Y) \leq \sum_{i=1}^{k} r(X_i) - (k - 1)r(X).$$

Fix a coding function f for cl. For any non-leaf v, the submodular inequality gives (with the sets $X_1, \ldots, X_k$ corresponding to $\{u, v\} : u \in c(v)$; and hence, $X = v$, $Y = v \cup c(v)$)

$$H_f(V) = H_f(c(v)) \le \sum_{u \in c(v)} H_f(u) - (|c(v)| - 1) H_f(v).$$

We first add up by level; for level k ($0 \le k \le L_t$) of tree T_t, we denote $H_k := \sum_{v \in l_k} H_f(v)$, and we obtain:

$$\frac{C_t!}{(C_t - k)!} H_f(V) \le H_{k+1} - (C_t - k - 1) H_k$$

$$\frac{C!}{(C_t - k)!} (C_t - k - 2)! H_f(V) \le (C_t - k - 2)! H_{k+1} - (C_t - k - 1)! H_k$$

Let us now add up for all levels:

$$\left[\sum_{k=0}^{L_t-1} \frac{C_t!}{(C_t - k)(C_t - k - 1)} \right] H_f(V) \le (C_t - L_t - 1)! H_{L_t} - (C_t - 1)! H_0$$

$$\le \frac{C_t!}{C_t - L_t} - (C_t - 1)! H_0,$$

where we used $H_{L_t} \le |l_{L_t}| = \frac{C_t!}{(C_t - L_t)!}$. Simplifying, we obtain:

$$L_t H(V) \le C_t - (C_t - L_t) H_0 = C_t - D(H - 1) H_f(R_t)$$

since, by definition, $H_0 = H_f(R_t)$. We now add up for all trees T_1 up to T_{r-1}, we obtain:

$$[D(r - 1) - D(H - 1)] H(V) \le DH(r - 1) - D(H - 1) - D(H - 1) \sum_{t=1}^{r-1} H_f(R_t), \qquad (1)$$

where we used the following relations:

$$\sum_{b=1}^{r-1} N_t = D(H - 1)$$

$$\sum_{b=1}^{r-1} L_t = D(r - 1) - D(H - 1)$$

$$\sum_{b=1}^{r-1} C_t = DH(r - 1) - D(H - 1).$$

Moreover, the set of all roots is a basis for the closure operator, hence:

$$H_f(V) = H_f(\{R_1, \ldots, R_r\}) \le 1 + \sum_{t=1}^{r-1} H_f(R_t). \qquad (2)$$

Multiplying (2) by $D(H - 1)$ and adding it with (1) eventually yields:

$$H_f(V) \le \frac{DH(r - 1)}{D(r - 1)} = H.$$

$\square$

We now construct the coding function with entropy H. Consider $A = B^D$, where B is any finite set of cardinality at least two. Any $x \in A^r$ can be expressed as $x = (x_1, \ldots, x_{rD}) \in B^{rD}$. For any subset $S \subseteq \{1, \ldots, rD\}$, say $S = \{i_1, \ldots, i_{|S|}\}$ once sorted in increasing order, we define the partition g_S of B^{rD} into exactly $|B^{|S|}|$ parts of equal size as:

$$P_y(g_S) := \{(x_{i_1}, \ldots, x_{i_{|S|}}) = y : y \in B^{|S|}\}.$$

We remark that $H(g_S) = |S|/D$. We shall assign a partition $f_v := g_{S(v)}$ to each vertex v; we only need to specify $S(v)$ for all v. Denoting $S(X) = \bigcup_{v \in X} S(v)$ for all $X \subseteq V$, we have $H_f(X) = |S(X)|/D$.

$S(v)$ is defined recursively for all trees, level by level. The set $S(R_t)$ for the root of tree T_t $(1 \le t \le r)$ is given by:

$$S(R_t) = \left\{1 + \sum_{s=1}^{t-1} N_s, \ldots, \sum_{s=1}^{t} N_s\right\}.$$

We denote $\Sigma := \{1, \ldots, DH\}$. Then, for any non-leaf v, the corresponding sets of its children are obtained by adding one element of Σ to $S(v)$; all added elements are distinct. That is, for all $u, u' \in c(v)$, we have:

$$S(u) \subseteq \Sigma$$
$$|S(u)| = |S(v)| + 1$$
$$S(u') \cap S(u) = S(v).$$

Let v be a non-leaf on level k. Since $|S(v)| = N_t + k$ and $|c(v)| = C_t - k = DH - N_t - k = |\Sigma| - |S(v)|$, we obtain $S(c(v)) = \Sigma$ for all non-leaves v.

Lemma 7. *The partitions f form a coding function for* cl *with entropy H.*

Proof. Let us prove that it is indeed a coding function for cl. Since $|S(v)| = N_t + k \le N_t + L = D$ for any v in level k of tree t, we obtain $H_f(v) \le 1$ for any $v \in V$. We then need to check that $S(X) = S(\mathrm{cl}(X))$ for any subset X of vertices. We first remark that if $v \in a(u)$, then $S(v) \subseteq S(u)$; hence $S(X) = S(a(X))$. This proves the claim when $\mathrm{cl}(X) = a(X)$. Otherwise, if $c(v) \subseteq a(X)$, then $\Sigma = S(c(v)) \subseteq S(a(X)) \subseteq S(X)$; if X intersects all trees, then $\Sigma = S(\{R_1, \ldots, R_r\}) \subseteq S(X)$. Finally, we have $S(V) = \Sigma$; hence, its entropy is equal to H. $\square$

5. Solvability of Operators

Since the closure solvability problem generalises different problems, we may be tempted to generalise it even further by consider operators that are not necessarily closures. In this section, we justify why we only need to focus on the closure solvability problem. Let us consider the most general way of defining the solvability problem.

Definition 10. *Let V be a finite set of n elements, $a : 2^V \to 2^V$, and A, B be finite sets (A is referred to as the alphabet, $|A| \ge 2$). A coding function for (a, A, B) is a tuple $f = (f_1, \ldots, f_n)$ of n partitions of B, where each partition is in at most $|A|$ parts, such that $f_{a(X)} = f_X$ for all $X \subseteq V$.*

We say that $a, a' : 2^V \to 2^V$ are equivalent if any tuple of partitions f is a coding function of a if and only if it is a coding function for a'.

Theorem 5. *Let $a : 2^V \to 2^V$; then, there exists a closure operator on V which is equivalent to a. Therefore, the solvability problem for a can be reduced to the solvability problem of some closure operator.*

Proof. We take three steps. Firstly, construct the digraph on 2^V with arcs $(Y, a(Y))$ for all $Y \subseteq V$. For any $X \subseteq V$, denote the connected component containing X as $C(X)$. Then, we claim that $b(X) := \bigcup_{Y \in C(X)} a(Y)$ is equivalent to a (we note that b is extensive). Indeed, if f is a coding function for a, then $f_X = f_{a(X)}$. Hence, for any $Y \in C(X)$, $f_Y = f_X$, and we obtain $f_{b(X)} = f_X$. Conversely, we have $b(X) = b(a(X))$; and hence, if f is a coding function for b, then $f_X = f_{b(X)} = f_{b(a(X))} = f_{a(X)}$ for all X.

Secondly, we claim that $c(X) := \bigcup_{Y \subseteq X} b(Y)$ is equivalent to b (we note that c is extensive and isotone). Indeed, if f is a coding function for b and $Y \subseteq X$, then f_X refines $f_Y = f_{b(Y)}$; thus, f_X refines $f_{c(X)}$. The converse is immediate; hence, $f_X = f_{c(X)}$, and f is a coding function for c. Conversely, if f is a coding function for c, then $f_X = f_{c(X)}$ refines $f_{b(X)}$ and, hence, is equal to $f_{b(X)}$ for all X.

Thirdly, we claim that $\mathrm{cl}(X) := c^n(Y)$ is equivalent to c (we note that cl is a closure operator). Indeed, if f is a coding function for c, then $f_X = f_{c(X)} = \ldots = f_{c^n(X)}$. Conversely, $f_X = f_{\mathrm{cl}(X)}$ refines $f_{c(X)}$. $\square$

6. Conclusions

In this paper, we pursued the study of closure solvability introduced in [8] for network coding and secret sharing.

We first investigated the nature of solvable closure operators. This yielded numerous new definitions (four different kinds of ranks) and a new criterion for non-solvability (Theorem 3). In passing, we give two new axioms for matroids in Theorems 1 and 2.

We then introduce the entropy of a closure operator, and we thoroughly investigate its properties. We are able to define the equivalent of the Shannon entropy of a graph. This yields Theorem 4, which shows that the set of entropy values of closure operators contains all rational numbers above one. However, it is easy to show that there are gaps between the entropy values of undirected graphs, for instance the only possible value between two and three is equal to 2.5. For directed graphs, we still do not know whether the set of entropy values is dense in $[1, \infty)$.

Conflicts of Interest

The author declares no conflict of interest.

References

1. Ahlswede, R.; Cai, N.; Li, S.Y.R.; Yeung, R.W. Network information flow. *IEEE Trans. Inf. Theory* **2000**, *46*, 1204–1216.
2. Li, S.Y.R.; Yeung, R.W.; Cai, N. Linear Network Coding. *IEEE Trans. Inf. Theory* **2003**, *49*, 371–381.
3. Riis, S. Linear versus non-linear Boolean functions in Network Flow. In Proceedings of 38th Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, 17–19 March 2004.
4. Dougherty, R.; Freiling, C.; Zeger, K. Insufficiency of linear coding in network information flow. *IEEE Trans. Inf. Theory* **2005**, *51*, 2745–2759.
5. Kötter, R.; Médard, M. An Algebraic Approach to Network Coding. *IEEE/ACM Trans. Netw.* **2003**, *11*, 782–795.
6. Ho, T.; Médard, M.; Kötter, R.; Karger, D.R.; Effros, M.; Shi, J.; Leong, B. A random linear network coding approach to multicast. *IEEE Trans. Inf. Theory* **2006**, *52*, 4413–4430.
7. Riis, S.; Ahlswede, R. Problems in network coding and error-correcting codes. In Proceedings of First Workshop on Network Coding, Theory, and Applications, Riva del Garda, Italy, 7 April 2005.
8. Gadouleau, M. Closure solvability for network coding and secret sharing. *IEEE Trans. Inf. Theory* **2013**, *59*, 7858–7869.
9. Riis, S. Utilising public information in network coding. In *General Theory of Information Transfer and Combinatorics*; Ahlswede, R., Baumer, L., Cai, N., Aydinian, H., Blinovsky, V., Deppe, C., Mashurian, H., Eds.; Lecture Notes in Computer Science, Volume 4123; Springer: Berlin/Heidelberg, Germany, 2006; pp. 866–897.
10. Riis, S. Information flows, graphs and their guessing numbers. *Electron. J. Comb.* **2007**, *14*, 1–17.
11. Körner, J. Coding of an information source having ambiguous alphabet and the entropy of graphs. In Proceedings of Transactions of the 6th Prague Conference on Information Theory, Statistical Decision Function, Random Processes, Prague, Czech Republic, 19–25 September 1971; pp. 411–425.
12. Lovász, L. On the Shannon Capacity of a Graph. *IEEE Trans. Inf. Theory* **1979**, *25*, 1–7.
13. Gadouleau, M.; Riis, S. Graph-Theoretical Constructions for Graph Entropy and Network Coding Based Communications. *IEEE Trans. Inf. Theory* **2011**, *57*, 6703–6717.
14. Christofides, D.; Markström, K. The Guessing Number of Undirected Graphs. *Electron. J. Comb.* **2011**, *18*, 1–19.
15. Brickell, E.F.; Davenport, D.M. On the Classification of Ideal Secret Sharing Schemes. *J. Cryptol.* **1991**, *4*, 123–134.
16. Matúš, F. Matroid representations by partitions. *Discret. Math.* **1999**, *203*, 169–194.
17. MacWilliams, F.J.; Sloane, N.J.A. *The Theory of Error-Correcting Codes*; North-Holland: Amsterdam, The Netherlands, 1977.
18. Birkhoff, G. *Lattice Theory*; American Mathematical Society: Providence, RI, USA, 1948.
19. Oxley, J.G. *Matroid Theory*; Oxford University Press: Oxford, UK, 2006.
20. Batten, L.M. Rank functions of closure spaces of finite rank. *Discret. Math.* **1984**, *49*, 113–116.

21. Gadouleau, M.; Goupil, A.   A Matroid Framework for Noncoherent Random Network Communications. *IEEE Trans. Inf. Theory* **2011**, *57*, 1031–1045.