Secret sharing on the infinite ladder

László Csirmaz
Central European University

Abstract
The notion of *perfect secret sharing scheme* has been extended to encompass infinite access structures, in particular infinite graphs, in [2]. The participants are the vertices of the graph G and the edges are the minimal qualified subsets. The *information ratio* of G is the largest lower bound on the amount of information by secret bits some vertex must receive in each scheme realizing this access structure. We show that this value is 7/4 for the infinite ladder, solving an open problem from [2]. We give bounds for other infinite graphs as well.

Key words: secret scharing scheme, information theory, infinite graph, information rate.

1 Introduction

In a *secret sharing scheme* some information is distributed among the participants so that qualified subsets of the participants, putting together their shares, can recover the secret. If, in addition, unqualified subsets gain no information wahtsoever on the secret, the scheme is *perfect.* Here we consider cases when the participants are the vertices of a (finite or infinite) graph, and minimal qualifies subsets are just the edges. The *information ratio* $R(G)$ of a finite graph G is the largest lower bound on the amount of information by secret bits (measured as Shannon entropy) some participant must remember in every scheme realizing this graph. If G is infinite, then $R(G)$ is the sup of $R(G')$ where G' is a finite spanned subgraph of G. For further motivation and exact definition, see [2].

In this paper we determine, or bound, the information ratio of several infinite graphs. The lower bounds use direct constructions and Stinson's decomposition technique from [3] generalized in [2]:

Theorem 1.1 *Let G_i be arbitrary (not necessary spanned) subgraphs of G, and assume that each edge of G is in at least k of the subgraphs. For each vertex $v \in G$ define $r_i(v) = 0$ if $v \notin G_i$, and $r_i(v) = R(G_i)$, i.e. the information ratio of G_i, otherwise. Then*

$$R(G) \le \sup_{v\in G} \frac{\sum r_i(v)}{k}. \quad \blacksquare \tag{1}$$

Upper bounds come from the so-called *entropy method*, see, e.g. [1]. For a detailed exposition please consult [2].

2 The ladder

In this section we show that information ratio for the infinite ladder L depicted on figure 1 is 7/4. We prove that this is an upper and also a lower bound for $R(L)$ separately.

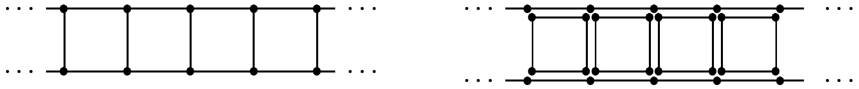

Figure 1: The ladder and its cover

Claim 2.1 $R(L) \le 7/4$.

Proof As all upper bounds, this one comes from a construction. Consider the right hand side of figure 1. The ladder is decomposed into two infinite paths and infinitely many squares. We will use theorem 1.1. Observe that all edges are covered exactly twice, i.e. $k = 2$. As the information ratio for the square is 1 and that of the infinite path is $3/2$ (see [2]), the sum in (1) is $2+3/2 = 7/2$ for each vertex v. This should be divided by $k = 2$ to get the upper bound $7/4$. ■

Claim 2.2 $R(L) \geq 7/4$.

Proof Rather than using the entropy method directly, we shall use the result of Theorem 2.3 below. We claim that the information ratio for the ladder is at least as much as that of the graph G_1 depicted on the left hand side of figure 2. Both G_1 and G_2 have ten vertices. On both cases vertices denoted by the same label are identical, the graphs on the picture are "unfolded" for an easier drawing. G_1 is the edge graph of the pentagonal prism, while G_2 is that of the pentagonal antiprism.

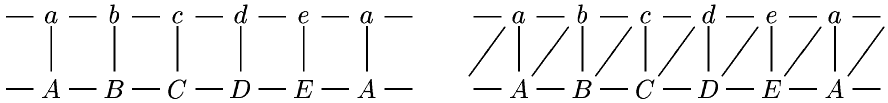

Figure 2: Graphs G_1 and G_2

Denote the information ratio of the infinite ladder L by $r = R(L)$. All finite spanned subgraphs of L has information ratio $\leq r$. In particular, consider the strip of length $5k$, consisting $5k-1$ squares put next to each other. Wrap this strip around G_1 like a ribbon. Each vertex of G_1 will be covered k or $k+1$ times, and each edge will be covered again k or $k+1$ times. We apply Theorem 1.1 with this "decomposition." The sum in (1) is either $k \cdot r$ or $(k+1)r$ for each vertex, and the denominator is k, thus

$$R(G_1) \leq \frac{k+1}{k} r.$$

As this holds for arbitrary large k, we must have $R(G_1) \leq r = R(L)$. Theorem 2.3 gives the lower bound $7/4$ for $R(G_1)$, thus we are done. ■

Theorem 2.3 *The information ratio is at least* $7/4$ *for both graphs* G_1 *and* G_2 *of figure 2.*

Proof The vertices $a, \ldots, e$ as well as vertices $A, \ldots, E$ form two cycles of length 5 in both graphs. In G_1 there are five other edges connecting vertices of these cycles as indicated on figure 2. In G_2 we have 10 edges between these cycles.

First we prove $R(G_1) \geq 7/4$. The proof uses the entropy method as described e.g., in [1, 2]. Let f be any non-negative submodular function with the strong submodulare property on the subsets of the vertex set of G_1. We must show that $f(v) \geq 7/4$ for some vertex $v \in G_1$. From now on fix such a function f. We proceed by stating and proving two lemmas.

Lemma 2.4 *Let* a, b, c, *and* d *be vertices of the graph* G *such that* ab, bc, cd *are edges,* ad *and* bd *are not edges (that is,* $abcd$ *is a spanned path of length* 3 *with* ac *as an optional extra edge). Suppose* $X \subseteq G$ *is independent, and no vertex in* X *is connected to any of* a, b, c, *or* d. *Then* $f(bcX) - f(X) \geq 3$.

Proof All standard proofs which give $f(bc) \geq 3$ can be extended to prove this stronger statement as well. For the sake of completeness, however, we give the details. Figure 3 shows the idea. Qualified (i. e. not empty) subsets are boxed. Among the four submodular inequalities indicated on the figure two are strong (where three out of the four subsets are qualified). Adding up this four inequalities we get

$$f(bcX) - f(X) \geq 2 + f(abcdX) - f(adX).$$

As $abcdX$ is qualified while adX is not, the last term on the right hand side is ≥ 1, which proves the lemma. ■

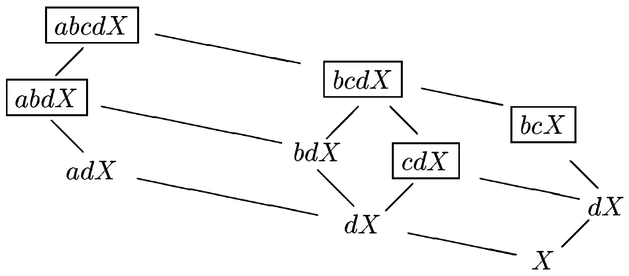

Figure 3: The proof

Lemma 2.5 *Let abc be a path in G, and $X \subseteq G$ be a subset of vertices such that acX is independent. Then $f(a)+f(b)+f(cX) \geq f(acX)+2$.*

Proof As ab and bc are both edges, strong submodularity gives $f(ab)+f(bcX) \geq f(b)+f(abcX)+1$. From here $f(a)+f(b)+f(cX) \geq f(abcX)+1$ follows. Now $abcX$ is qualified and acX is not, thus $f(abcX) \geq f(acX)+1$, which proves the lemma. ▮

Returning to the proof of $R(G_1) \geq 7/4$, in G_1 acD is independent, abc is a path, therefore, by Lemma 2.5,

$$f(a)+f(b)+f(cD) \geq f(acD)+2.$$

Similarly, ADc is independent, and AED is a path, thus

$$f(A)+f(E)+f(cD) \geq f(AcD)+2.$$

By submodularity,

$$f(acD)+f(AcD) \geq f(aAcD)+f(cD).$$

Addig these inequailities we have

$$f(a)+f(b)+f(A)+f(E) \geq 4+\big(f(aAcD)-f(cD)\big) \geq 4+3=7, \tag{2}$$

where the last inequality comes from Lemma 2.4. Indeed, in G_1, $eaAB$ is a spanned path no vertices of which is connected to the independent set cD. (2) means that at least one of $f(a)$, $f(b)$, $f(A)$, and $f(E)$ is $\geq 7/4$ which proves the theorem for G_1.

In G_2 both eab and bcd are spanned paths, thus applying Lemma 2.5 with X as the empty set we have $f(e)+f(a)+f(b) \geq f(eb)+2$, and $f(b)+f(c)+f(d) \geq f(bd)+2$. By submodularity, $f(eb)+f(bd) \geq f(bde)+f(b)$. Combining these inequalities one gets

$$f(e)+f(a)+f(c)+f(d) \geq 4+\big(f(bde)-f(b)\big) \geq 4+3=7. \tag{3}$$

Again, the last inequality is a consequence of Lemma 2.4, as no vertex in the spanned path $CdeE$ is connected to b. By (3) at least one of the four values on the left hand side is $\geq 7/4$, as required. ▮

3 Further examples

Using the methods and results from the previous section, we can bound the information ratio of other infinite graphs as well. Figure 4 shows two infinite ladder-like constructs, L_1 and L_2. In both graphs the vertices lie on the two infinite paths, and vertices on these paths are connected as indicated. In L_1 each vertex has degree 4, while in L_2 this degree is 5. Graphs H_1, H_2 and H_3 on the righ hand side of the figure will be used for upper bounds.

Example 3.1 *The information ratio of L_1 is $3/2$.*

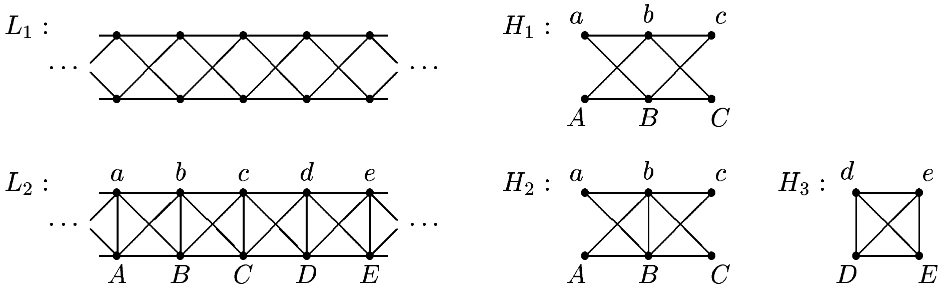

Figure 4: Variants on the ladder: L_1 and L_2 and their covers

Proof L_1 contains the infinite path as a spanned subgraph, consequently the ratio is at least the ratio of the path, which is $3/2$. To show that $3/2$ is also an upper bound, cover L_1 with translated instances of H_1 and apply Theorem 1.1. Each edge of L_1 will be covered exactly twice, thus $k = 2$ in the theorem. Each vertex on the upper path will be covered once by a, once by b, and once by c; and similarly vertices on the bottom path receive each of A, B, and C exactly once. Thus to prove the claim it is enough to show that there exists a perfect secret sharing scheme on H_1 which assigns a single bit to each node for each secret bit. Indeed, in this case the sum in (1) is always 3 which should be divided by $k = 2$ yielding the upper bound $3/2$.

As for H_1, observe that it is a complete bipartite graph with bB and $aAcC$ as the two classes. In this case a perfect secret sharing scheme realizing the minimal ratio 1 is the following. Let $s \in \{0,1\}$ be the secret bit, and choose $r \in \{0,1\}$ randomly. Give r to all members of one class, and $r \oplus s$ to members of the other class. ∎

Example 3.2 *The information ratio of L_2 is $5/3$.*

Proof The lower bound comes from the entropy method. Let $abcde$ be five consecutive vertices on the top path as indicated on the figure, and let $ABCDE$ be the vertices just below them. By Lemma 2.5,

$$f(a) + f(b) + f(c) \geq f(ac) + 2,$$

and, by Lemma 2.4, $f(acd) \geq f(a) + 3$. This latter inequality follows as a, as a single element set, is independent, and no vertex in the path $Ccde$ is connected to a. ($Ccde$ is not a spanned path, but the only extra edge Cd is allowed in the Lemma.) Now $f(ac) + f(d) \geq f(acd)$, therefore

$$f(b) + f(c) + f(d) \geq 5,$$

that is one of these three values must be $\geq 5/3$.

The upper bound uses Theorem 1.1. We shall cover L_2 by translated instances of H_2 and H_3. Both H_2 and H_3 has information ratio 1. Indeed, complete graphs have this ratio, and H_3 is the complete graph on 4 vertices. In H_2 use a ratio 1 secret sharing system on the triangle abB, and then simply give a's share to A, c and C.

Put H_2 and H_3 to all possible positions in L_2. Each edge will be covered 3 times, and each vertex 5 times. Thus all vertices receive a total of 5 bits, which should be divided by 3 to get the upper bound. ∎

Example 3.3 *For the "reinforced ladder" L^* of figure 5,* $7/4 \leq R(L^*) \leq 11/6$.

Observe that L^* is isomorphic to a strip of width 1 cut out of the triangular lattice.

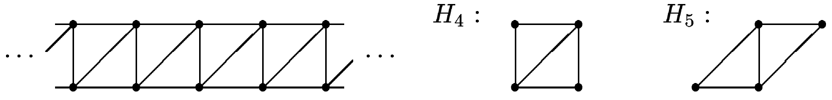

Figure 5: The "reinforced ladder" L^* and the cover graphs

Proof The lower bound comes from the $R(G_2) \geq 7/4$ part of Theorem 2.3 the same way as the other claim in the same theorem was used to get a lower bound on the information ratio of the infinite ladder.

For the upper bound consider the graphs H_4 and H_5 depicted on figure 5. Both H_4 and H_5 have information ratio 1. Cover L^* by the translated copies of H_4 and H_5. Each vertex will be covered 4 times, horizontal edges (i.e. edges on the two infinite paths) will be covered twice, while all other edges will covered three times. Add the upper and lower infinite path to make the edge cover exactly 3 everywhere. The sum of the ratios at each vertex is increased by the information ratio of the infinite path, which is 3/2. Thus the upper bound ensured by Theorem 1.1 is $(4+3/2)/3 = 11/6$ as was claimed. ▮

4 Conclusion

We have determined the information ratio (thus the information rate as well) of three infinite graphs, and gave estimates for a fourth one. In each case the upper bound was achieved by Stinson's decomposition method generalized for infinite graphs. The lower bounds used the entropy method. In two cases, however, it was done with a twist: rather than applying the method directly, we gave lower bounds for a finite "factor graph," and then argued that the information ratio of the original graph is at least as large as that of its factor. What we have lost in this argument is the locality. It is quite conceivable that all finite parts of the graph has strictly smaller information ratio than the whole graph. Thus, while we have established the information ratio of the infinite ladder, it remains open whether the same ratio is achieved by a finite spanned subgraph.

Graphs L_1 and L_2 are *local.* We know that the path of lenght 3 has information ratio 3/2, and this is a spanned subgraph of L_1. From the proof of Example 3.2 and Lemmas 2.4 and 2.5 one can extract that the graph depicted on figure 6, with or without any of the dotted edges, has information ratio 5/3. One of these graphs is a spanned subgraph of L_2, thus L_2 is local.

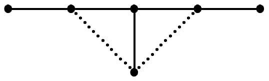

Figure 6: A graph with information ratio 5/3

References

[1] C. Blundo, A. De Santis, D. R. Stinson, U. Vaccaro: Graph Decomposition and Secret Sharing Schemes *Journal of Cryptology,* Vol 8(1995) pp. 39–64.

[2] L. Csirmaz: Secret sharing on infinite graphs, preprint – available as IACR eprint `http://eprint.iacr.org/2007/297`

[3] D. R. Stinson: Decomposition construction for secret sharing schemes, *IEEE Trans. Inform. Theory* Vol 40(1994) pp. 118-125.