Minimal Selectors and Fault Tolerant Networks

O. Amini[a], F. Giroire[b], F. Huc[a*] and S. Pérennes[a]
[a] Projet Mascotte (CNRS, INRIA, UNSA), INRIA Sophia-Antipolis,
2004 route des Lucioles BP 93, 06902 Sophia-Antipolis Cedex, France
[b] Projet Algorithmes, INRIA Rocquencourt,
F-78153 Le Chesnay, France

Abstract

In this paper we study a combinatorial optimization problem issued from on-board networks in satellites. In this kind of networks the entering signals (inputs) should be routed to amplifiers (outputs). The connections are made via expensive switches with four links available. The paths connecting inputs to outputs should be link-disjoint. More formally, we call $(p, \lambda, k)-$*network* an undirected graph with $p + \lambda$ inputs, $p + k$ outputs and internal vertices of degree four. A $(p, \lambda, k)-$network is *valid* if it is tolerant to a restricted number of faults in the network, i.e. if for any choice of at most k faulty inputs and λ faulty outputs, there exist p edge-disjoint paths from the remaining inputs to the remaining outputs. In the special case $\lambda = 0$, a $(p, \lambda, k)-$network is already known as a *selector*.

Our optimization problem consists of determining $N(p, \lambda, k)$, the minimum number of nodes in a valid $(p, \lambda, k)-$network. For this, we present validity certificates and a gluing lemma from which derive lower bounds for $N(p, \lambda, k)$. We also provide constructions, and hence upper bounds, based on expanders. The problem is very sensitive to the order of λ and k. For instance, when λ and k are small compared to p, the question reduces to avoid certain forbidden local configurations. For larger values of λ and k, the problem is to find graphs with a good expansion property for small sets. This leads us to introduce a new parameter called α-*robustness*. We use α-robustness to generalize our constructions to higher order values of k and λ. In many cases, we provide asymptotically tight bounds for $N(p, \lambda, k)$.

Keywords: concentrators, superconcentrators, fault tolerant networks, switching networks, routing, expanders, connectivity, disjoint paths.

*Florian Huc is partialy supported by Région Provence Alpes Côte d'Azur. This work has been partially funded by the European Community project IST FET AEOLUS

1 Introduction

Motivation. One of the most fundamental questions in many applications of computer science and graph theory is the design of *efficient networks*. Efficient can have several meanings depending on the context. Properties such as high connectivity, fault tolerance and being algorithmically simple are at the heart of such properties. In this paper we study a combinatorial optimization problem of this kind. The problem, originally posed by *Alcatel Space Industry*, comes from the design of efficient on-board networks in satellites (also called Traveling Wave Tube Amplifiers). For example, the satellites under consideration are used for TV and video transmission (like the Eutelsat or Astra series) as well as for private applications. Signals incoming in a telecommunication satellite through ports have to be routed through an on-board network to amplifiers. A first constraint is that the network is built of switches with four links. But other constraints appear. On the one hand the amplifiers may fail during the satellite's life time and can not be repaired. On the other hand, as the satellite is rotating on itself, not all the ports and amplifiers are well oriented and hence available. So more amplifiers and ports are needed than the number of signals which have to be routed. One can easily construct a network fulfilling these constraints by using two concentrators of any fixed degree. However, to decrease launch costs, it is crucial to minimize the network physical weight, i.e. for us, to minimize the number of switches. Since switches are also expensive to build, it is worth saving even one. Space industries are interested in designing such networks for specific values of the parameters. However the general theory is of interest by itself.

Problem. We consider here *networks*, connecting a set of *inputs* to a set of *outputs*. A network can be seen as a graph with a set of inputs and outputs, vertices of this graph representing the switches. We define a $(p, \lambda, k)-$*network* as a network with $p + \lambda$ inputs and $p + k$ outputs. A $(p, \lambda, k)-$network is said to be *valid*, if it can tolerate up to k faults in inputs and up to λ faults in outputs, more formally if for any choice of p inputs and of p outputs, there exist p edge-disjoint paths linking all the chosen inputs to all the chosen outputs. By symmetry, we may assume in the following that $k \geq \lambda$ and we set $n := p + k$.

Note that finding minimal networks is a challenging problem and even testing the validity of a given network is hard (see related work). We study the case where the switches of the network have degree four (although the theory can be generalized to any degree) which is of primary interest for the applications. The problem is to find $N(p, \lambda, k)$, the minimum number of switches in a valid $(p, \lambda, k)-$network and to give constructions of such networks.

Related Work. This study of a new kind of network should be considered in the spirit of the well studied theory of *superconcentrators*. A $(p+k, p)$-*concentrator* [Val75] is a directed acyclic graph $G = (V, E)$ with $p+k$ designated input nodes and p designated output nodes ($k \geq 0$), such that for each subset of p input nodes, there exist p edge-disjoint (or, depending on the context, vertex-disjoint) paths from the input nodes to the output nodes. A *selector*, first introduced in [BDD02], is a $(p, 0, k)$-network ($\lambda = 0$). A general theory of selectors can be found in [BPTed], where several results are obtained for small values of k. A selector can be seen as an undirected version of a $(p+k, p)$-concentrator. An *n-superconcentrator* [Pip77] is a directed acyclic graph $G = (V, E)$ with n designated input nodes and n designated output nodes such that, for any set S of $p \leq n$ inputs and any set T of p outputs, there exist p edge-disjoint (or, node-disjoint depending on the context) paths connecting S to T. There is a vast theory of superconcentrators (See the seminal work of Pippenger [Pip77] for an introduction, [AM84, AGM87, AC03] and Schöning [Sch06] for constructions, and [BKP$^+$81] for complexity issues).

In this way, (p, λ, k)-networks generalize the concept of selectors as superconcentrators generalize concentrators. It is also clear that taking a superconcentrator (resp. $(p+k, p)-$concentrator) and forgetting the orientations provides a valid (p, λ, k)-network (resp. selector) for every value of $k = \lambda$ (resp. any k and $\lambda = 0$). So one can try to use superconcentrators to construct efficient on-board satellite networks, but, not surprisingly, this does not give minimal networks in general. The major difference between the superconcentrators and general valid networks is that in a valid network the number of inputs and outputs that may become out of service is bounded (in our case, given a failure probability, no more that k failures will occur during the satellite lifetime) To find a minimal network (a superconcentrator of low density or having a minimum number of vertices) is a challenging problem and is an active area of research (see the papers [AM84], [AGM87], [AC03] and very recent construction in [Sch06]). From algorithmic point of view, one can show that the problem of testing if a graph is a $(p+k, p)$-concentrator or a superconcentrator, is coNP-complete. In fact, they are complete even when restricted to the important special case of graphs of size linear in the number of inputs (see [BKP$^+$81]). By the same arguments one can prove that the problem of deciding if a given (p, λ, k)-network is valid or not is coNP-complete, even restricted to the networks of regular degree 4.

In [BHT06] the authors consider a variant of selectors where some signals have priority and should be sent to amplifiers offering the best quality of service. In [BD02] the authors study the case were all the amplifiers are different and where a given input has to be sent to a dedicated output. This problem is related to permutation networks.

In [BGP06], the authors present exact values of $N(p, \lambda, k)$ for small values of k and λ and arbitrary values of p. For instance $N(p, 2, 1) = N(p, 1, 2) = N(p, 2, 2) = p + 2$ and also for $k \in \{3, 4\}$ and $0 < \lambda \leq 4$, $\mathcal{N}(p, \lambda, k) = \lceil \frac{5n}{4} \rceil$

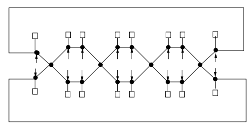

Figure 1: A valid (12,4,4)-network

Results. We are primarily interested in this paper in *large networks*, where $n = p + k$ tends to infinity and also k is large enough. We present several upper and lower bounds for the minimal number of switches in a valid $(p, \lambda, k)-$network. In many cases these bounds are asymptotically tight. Since forgetting the orientation of superconcentrators provide valid $(p, \lambda, k)-$networks, these results, as far as we know, provide the first lower bounds on the size of a superconcentrator. To obtain the lower bounds we present a very powerful technique, *quasi-partitioning.* We give here the very first applications of this lemma, but we think it may have several applications in other related problems (for example bisection-width, see [MP01]).
To obtain upper bounds we propose several constructions. The construction of optimal valid networks will heavily rely on *expanders* (see section A.2) . Using these, we are able to construct simplified networks with $2n$ switches as soon as n is large enough and $k \leq c_1 \log n$ for some constant c_1 (Section 3.1). In Section **??** we also give a lower bound of order $2n(1 - \epsilon(k))$ where $\epsilon(k)$ tends to zero when k tends to infinity (but we do not need $k \leq c_1 \log n$). Thus for simplified networks the problem is asymptotically solved for $k \leq c_1 \log n$. For general networks, using bipartite expanders, we obtain an upper bound of $n + \frac{3}{4}n$ when $k \leq c_2 \log n$ for some constant c_2. The lower bound we obtain is $(n + \frac{2}{3}n)(1 - \epsilon(\lambda, k))$, and we conjecture that $n + \frac{3}{4}n$ should be the right value. We also give a construction of selectors (case $\lambda = 0$) of size $n + \frac{n}{2}$, in which case we get also a tight lower bound.
To extend the results to larger values of k, we define a local expansion property of graphs that we call $\alpha-$*robustness* (see [CRVW02, AHK99] for some related notions). Intuitively, $\alpha-$robustness of a graph G, is a local version of

expansion factor. It is the maximum integer r_α such that for small subsets the expansion factor is α but for larger subsets, the minimum number of outgoing edges is asked to be at least r_α. In our constructions, we only need our graph to be an expander for small subsets, but for larger subsets all we need is a minimum constant edge-connectivity to the rest of the graph. This notion is also interesting by its own sake and contains as particular case several expansion invariants as bisection-width and Cheeger's constant (see [Chu97]). As random graphs are very good expanders, we study the $\alpha-$robustness of random graphs. In this way we generalize Bollabàs's result on expansion factor of random 4-regular graphs(see [Bol88]) to obtain related results for $\alpha-$robustness of random 4-regular graphs. As far as we know it is the first time in the literature that this new concept of local expanders are defined and investigated. Using this we present a construction of valid $(p,\lambda,k)-$networks with $3n$ switches for $\lambda \leq k \leq \frac{n}{7}$.

2 Preliminaries

In this section, we define more formally the design problem and introduce notations used throughout the paper. We state a cut criterion (Proposition 1): this criterion is fundamental because it characterizes the validity of $(p,\lambda,k)-$networks. It is extensively used to prove that networks are valid.

In Section 5 we use the cut criterion to detect forbidden patterns leading to lower bounds for the number of switches of valid networks. Proofs of lower and upper bounds are simplified by the use of last notion introduced here, the *associated graph* of a network (see Section A.3 and Section 5.1).

Notations. Given a function f, we define $f(A) := \sum_{a\in A} f(a)$ for any finite set A. For a subset W of vertices of a graph $G = (V,E)$, let us denote by $\Delta(W)$ the set of edges connecting W and $\overline{W} = V\backslash W$ and by $\Gamma(W)$ the set of vertices of $\overline{W}$ adjacent to a vertex of W. If a set is denoted by an upper case letter, the corresponding lower case letter denotes its cardinality ($\delta(W) = |\Delta(W)|$).

$(p,\lambda,k)-$**networks and valid** $(p,\lambda,k)-$**networks.** A $(p,\lambda,k)-$*network* is a triple $\mathcal{N} = \{(V,E),i,o\}$ where (V,E) is a graph and i,o are positive integral functions defined on V called input and output functions, such that for any $v \in V$, $i(v) + o(v) + deg(v) = 4$. The total number of inputs is $i(V) = \Sigma_{v\in V} i(v) = p + \lambda$, and the total number of outputs is $o(V) = \Sigma_{v\in V} o(v) = p+k$. We can see a network as a graph where all vertices but the leaves have degree 4, in which inputs and outputs are leaves. A *non-faulty output function* is a function o' defined on V such that $o'(v) \leq o(v)$

for any $v \in V$ and $o'(V) = p$. A *used input function* is a function i' defined on V such that $i'(v) \leq i(v)$ for any $v \in V$ and $i'(V) = p$. A (p, λ, k)-network is said *valid* if for any non-faulty output function o' and any used input function i', there are p edge-disjoint paths in G such that each vertex $v \in V$ is the initial vertex of $i'(v)$ paths and the terminal vertex of $o'(v)$ paths.

Design Problem. Let $N(p, \lambda, k)$ denotes the minimum number of switches of a valid (p, λ, k)-network. The *Design Problem* consists in determining $N(p, \lambda, k)$ and in constructing a minimum (p, λ, k)-network, or at least a valid (p, λ, k)-network with a number of vertices close to the optimal value. We introduce a variation of the problem, the *Simplified Design Problem*, which is to find minimum networks having $p+\lambda$ switches, each of them with one input and one output, and with $k - \lambda$ switches with only one output. Networks of this kind are especially good for practical applications, as they simplify the routing process, minimize path lengths and lower interferences between signals.

Excess, Validity and Cut-criterion. To verify if a network is valid, instead of solving a flow/supply problem for each possible configuration of output failures and of used inputs, it is sufficient to look at an invariant measure of subsets of the network, the *excess*, as expressed in the following proposition.

Proposition 1 (Cut Criterion) *A* $(p, \lambda, k)-$*network is* valid *if and only if, for any subset of vertices* $W \subset V$ *the* excess of W*, defined by,*

$$\varepsilon(W) := \delta(W) + o(W) - \min(k, o(W)) - \min(i(W), p),$$

satisfies $\varepsilon(W) \geq 0$.

The intuition is that the signals arriving in W (in number at most $\min(i(W), p)$) should be routed either to the valid outputs of W (in number at least $o(W) - \min(k, o(W))$) or to the links going outside (in number $\delta(W)$). The omitted formal proof reduces to a supply/demand flow problem. Remark that, for the cut criterion, it is sufficient to consider only connected subsets W with connected complement $\overline{W}$ (This comes from the submodularity of ε).

Associated Graph Vertices $D \in V$ of degree 2 with $i(D) = o(D) = 1$ play an important role. We call them *doublon*. A switch that is not a doublon is called an *R-switch*. Remark that for $k \geq 3$ no paths has 3 or more consecutive doublons. Indeed if we consider the set W consisting of these doublons we have $\delta(W) = 2$ and $o(W) = i(W) \geq 3$. The cut criterion would give a contradiction.

Let $\mathcal{N}$ be a $(p, \lambda, k)-$network. We build a *graph* $\mathcal{R}$ *associated to* $\mathcal{N}$. Its vertices are the R-switches of $\mathcal{N}$. Consequently the edges of $\mathcal{R}$ are of three kinds, respectively E_0, E_1 and E_2: the edges of $\mathcal{N}$ between two $R-$switches, the edges corresponding in $\mathcal{N}$ to a path of length 2 with a doublon in the middle and those corresponding to a path of length 3 with 2 doublons in the middle.

3 Upper Bounds: The design problem

In this section, we present three constructions with $2n$, $n + \frac{3}{4}n$ and $n + \frac{n}{2}$ switches respectively for the simplified design problem, the design problem (any λ) and for the design problem when $\lambda = 0$. All these constructions are valid for $k \leq c \cdot \log n$ (where c is a constant depending only on the expansion factor of 3 and $4-$regular graphs).

3.1 Simplified Design Problem - Upper Bound $2n$

In this subsection, we use the existence of expanders presented in subsection A.2 to construct valid $(p, \lambda, k)-$networks with $2n = 2(p+k)$ switches for large n and $k \leq c_1 \log n$ (c_1 depending on the expansion factor of $4-$regular expanders, $c_1 = \frac{1}{6}$ when using explicit Ramanujan graphs). Furthermore we will show in Section 5 a lower bound of the same order for the simplified design problem.

Theorem 1 *Let $n = p + k$, $k \leq \frac{1}{6} \log n$, for n large enough, we have: $N(p, k, k) \leq 2n$.*

Proof. The results for expanders exposed in Section A.2 state the existence of $(n, 4, c = \frac{1}{4})-$E-expander, $G = (V, E)$, of girth g, $g \geq \frac{2}{3} \log n$. Let $k \leq c \cdot g$ and $p = n - k$. It is well known that in a $4-$regular graph there exists a family of vertex disjoint cycles covering all vertices of G. Let us call this family F and add n new vertices by subdividing each edge of F into two edges. On each new vertex, we add an output and input creating a doublon. We now have a $(p, k, k)-$network, $\mathcal{N}$, with $2n$ switches. The proof of validity of this network is given in Appendix A.3. $\square$

We can derive $(p, \lambda, k)-$networks for any $\lambda \leq k$ by deleting $k - \lambda$ inputs.

3.2 Design Problem - Upper Bound $n + \frac{3}{4}n$

In this subsection, we construct general $(p, k, k)-$networks for large n, $k \leq c_2 \log n$ (where c_2 depends on the expansion factor of $3-$regular expanders). We can also derive $(p, \lambda, k)-$networks for any $\lambda \leq k$ by deleting $k - \lambda$ inputs. Theorem 2 gives a $n + \frac{3}{4}n$ upper bound for such networks. Constructions are based on 3-regular bipartite expanders.

Definition 1 Two edges are at distance d *if any path that contains both of them is of length at least* $d + 2$. A node is at distance d of an edge *if any path that contains both of them is of length at least* $d + 1$.

Lemma 1 *Let G be a $3-$regular bipartite graph $G = (V_1 \cup V_2, E)$ of large girth ($g = \Theta(\log |V_1|)$) which is an $(2|V_1|, 3, c)$-E-expander and suppose $2k \leq cg$. Let $\mathcal{F}$ be a set of selected edges, such that any two edges of $\mathcal{F}$ are at distance at least 3. The network $\mathcal{N}$ obtained from G by adding a doublon on each edge of $\mathcal{F}$, an input on each vertex of V_1 and an output on each vertex of V_2 is a valid network.*

The proof is given in Appendix A.3.

Theorem 2 *(Construction) Let $n = p+k$, $k \leq \frac{1}{15} \log n$, for n large enough, we have: $N(p, k, k) \leq n + \frac{3}{4}n$*

Proof. Take $H = (A, B, E)$, a bipartite $(2|A|, 4, c')$-E-expander with girth $g = \frac{4}{3} \log n$. Let k, $k \leq c' \cdot g \leq \frac{4}{3} \log n$ (for existence see Section A.2). Take a complete matching F in the bipartite complement $\overline{H} = (A, B, \overline{E})$ of H, that is, if $(u, v) \in F$, then $u \in A$, $v \in B$ and u, v are not adjacent in H. For each edge $e = (a, b)$ of F, replace a and b by three vertices a_1, a_2, a_3 and b_1, b_2, b_3, add edges (a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1) and (a_3, b_1). Finally join a_2 (resp b_2) to two neighbors of a (resp b) and a_3 (resp b_3) to the two others neighbors. See Figure 2. We obtain a $3-regular$ bipartite graph G, $(6|A|, 3, \frac{c}{5}) - E-$expander. Note that by construction the edges of type (a_1, b_1), with $(a, b) \in F$ form a selected set $\mathcal{F}$ of edges pairwise at distance 3. We can apply Lemma 1 to G with $\mathcal{F}$ as selected set. All together we have $6|A| + |\mathcal{F}| = 7|A|$ switches, $|V_1| + |\mathcal{F} = 4|A|$ inputs, $|V_2| + |\mathcal{F} = 4|A|$ outputs. So, with $n = p + k$, $N(p, \lambda, k) = 7|A| = \frac{7}{4}n$ □

3.3 Design Problem: $\lambda = 0$ - Upper Bound $n + \frac{n}{2}$

In this subsection, we study selectors (the case $\lambda = 0$). In Theorem 3 we construct valid $(p, 0, k)-$networks with $n + \frac{n}{2}$ switches for n large and $k \leq$

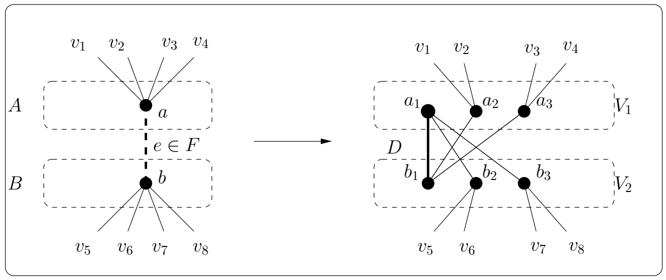

Figure 2: 'Expansion' of a selected couple of a bipartite graph (A, B, E).

$c_3 \log n$ (c_3 depends on the expansion factor of 3-regular expanders). Such networks are built from bipartite 3−regular vertex-expanders (see Appendix A.2).

Theorem 3 *Let $n = p + k$, $k \leq \frac{1}{48} \log_2 n$, for n large enough, we have:*

$$N(p, 0, k) \leq n + \frac{3}{4}n$$

Proof. Let us take $G = (V_1, V_2, E)$ a bipartite $(n, 3, d = \frac{1}{12}) - V-$expander of large girth $g \geq \frac{4}{3} \log n$(for existence see Section A.2). Let $\alpha = \frac{4}{d} = 48$ and k such that $k \leq d \cdot \frac{g}{2} \leq \frac{g}{12}$ and $k.(2^{\alpha k} + 1) \leq n$.

To each vertex of V_1, we connect a node with one input and two outputs. Such a switch is said to be of type T. To each vertex of V_2, we connect an input. We choose a subset S of k nodes in V_2 such that the distance between any two of them is at least $\alpha \cdot k$ (see Definition 1). By the choice of k we can choose the nodes in S one by one after removing all the nodes at distance less than αk of already chosen nodes (at each step we remove at most $2^{\alpha k} + 1$ new nodes). We remove the inputs of all nodes of S obtaining a $(p = n - k, 0, k)-$network that we call $\mathcal{N} = (V, E, i, o)$. The proof of validity of $\mathcal{N}$ is given in Appendix A.3. □

4 Graph Robustness: A new approach to the design of valid networks

The construction of valid networks is related to a more general expansion property of graphs, especially to what can be seen as a 'bounded expansion property' or expansion property only for sets of bounded size. We call this property *robustness*.

Definition 2 *(α-robustness) The α-robustness, rob_α of a graph G is the maximum value r, such that for every subset $X \subset V(G)$ with $|X| \leq \frac{|X|}{2}$ we have $\delta(X) \geq \min(r, \alpha|X|)$*

For $\alpha = 1$ we just say robustness. There are two main problems: on one hand we want to understand the behaviour of the robustness for a general graph, which means giving some upper bounds, for instance showing the existence of subsets which violate the $\alpha-$robustness. This problem covers in particular the problem of bisection-width, studied by several authors (see for example [Alo93] and [MP01]), which has several important applications. On the other hand for many applications one would like to be able to find graphs of large robustness ($\alpha-$robustness). First examples of such graphs are expanders of expansion factor c which give graphs with $c-$robustness equal to $\frac{n}{2}$ where n is the number of vertices. For d-regular graphs we have:

- If G is d-connected, $rob_d = 1$ and $rob_{d-1} = 2$. $rob_{d-2} = g$ where g is the double girth of the graph (minimum size of a cycle with a chord).
- for $\alpha \leq \frac{1}{2}(d - 2\sqrt{d-1})$, $rob_\alpha(G) = \frac{n}{2}$ for Ramanujan graphs.
- for $\alpha > \frac{d}{2} - c\sqrt{d}$ where c is some absolute constant depending only on d, $\alpha-$robustness is strictly smaller than $\frac{n}{2}$.(see Alon [Alo93])
- for $\alpha > \frac{1}{3} + \epsilon$ the $\alpha-$robustness of a 3-regular graph is strictly smaller than $\frac{n}{2}$, the same is true for $\alpha > \frac{4}{5} + \epsilon$ and for 4-regular graphs (see Monien-Preis [MP01])

Remark that since it is NP hard to compute double girth of a graph, computing $rob_2(G)$ is an NP hard problem. The same is true for any α.

4.1 Robustness of random 4-regular graphs

In this section $\mathcal{G}(k,n)$ is the probability space of all graphs on n vertices that are the union of k disjoint Hamiltonian cycles, all graphs occurring with same probability. By $G_{k,n}$ we denote an element of $\mathcal{G}(k,n)$. This probability space is equivalent to the probability space of random $2k$-regular graphs [GKW04].

Theorem 4 *Random 4-regular graphs have 1-robustness $\frac{n}{14}$ with high probability.*

Proof. (Sketch, more details can be find in appendix) Let G be a graph of $\mathcal{G}(k,n)$ and S a subset of V with s vertices. On the cycles $C_1, C_2, \ldots C_k$ constituting G, S can be described as a set of continuous intervals. For $i = 1, \ldots k$, let $m_i(S)$ be the number of intervals that S defines on C_i. Then $\delta(S) = 2\sum_{i=1,2,\ldots k} m_i(S)$

For a given cyclic permutation π, if $I(s,m)$ denotes the number of sets of s elements defining m segments on the cycle associated to π, we have:

$$I(s,m) = \binom{s-1}{m-1}\binom{n-s}{m} + \binom{n-s-1}{m-1}\binom{s}{m} = \binom{s}{m}\binom{n-s}{m}\left(\frac{m}{s} + \frac{m}{n-s}\right) \tag{1}$$

Given a random cyclic permutation π, we denote by $P(s,m)$ the probability that a set S with s elements defines m segments on the cycle associated to π. Since the probability does not depend on S, but only on s, $P(s,m)$ is well defined. We have:

$$P(s,m) = I(s,m)/\binom{n}{s} = \frac{\binom{s}{m}\binom{n-s}{m}\left(\frac{m}{s} + \frac{m}{n-s}\right)}{\binom{n}{s}} \tag{2}$$

$$Prob(\delta(S) = 2x) = \sum_{k_1,\ldots,k_k | k_1+k_2+\ldots+k_k = x} \Pi I(s,k_i)/\binom{n}{s}^k \tag{3}$$

We say a set is *bad* if $\delta(S) < min(s, n-s, r)$. By the above equations we can estimate the probability of having bad sets. The following two lemmas finally complete the proof of our Theorem.

Lemma 2 (Robustness for small sets) *For n large enough any set with size $s \leq \frac{n}{14}$ has border at least s with probability $u > 1/2$.*

Lemma 3 (Robustness for large sets) *For n large enough any set with size $s \in [\frac{n}{14}, \frac{13n}{14}]$ has border at least $\frac{n}{14}$ with probability $u > 1/2$.*

□

Remark 1 *The same method can be used to obtain lower bounds for α-robustness for random 4-regular graphs. Here is some numerical results for some special values of α.*

- $r_{\frac{11}{25}} = \frac{n}{2}$ *(See Bollobàs [Bol88] for another proof of this result).*

- $r_{\frac{11}{20}} \geq \frac{n}{2.6}$, $r_{\frac{4}{5}} \geq \frac{n}{5.7}$, $r_{\frac{2}{3}} \geq \frac{n}{3.6}$, $r_{\frac{3}{5}} \geq \frac{n}{3}$.

Using the concept of graph robustness we can extend the results of last section:

Theorem 5 *(cf proof in Appendix) For $k \leq \frac{n}{7}$ there exist $(p, \lambda, k)-$valid networks of size $3n$.*

5 Lower Bounds

In subsection 5.1, we prove a fundamental preliminary theorem, Theorem 6. Its main point is that $N(p, \lambda, k) \geq \frac{3}{2}n + \frac{d}{2} - \varepsilon(n)$ (where $\varepsilon(n)$ tends to zero when n tends to infinity). Direct applications of this theorem give lower bounds for general and simplified networks (Theorems 7, 8). We succeed in obtaining a better bound of $n + \frac{2}{3}n - \varepsilon(n)$ for two cases: when λ goes to infinity (Theorem 9) and when some kinds of switches are not allowed in the networks (Theorem 10). Finally (Theorem 11), we increase the bound to $n + \frac{3}{4}n - \varepsilon(n)$ for another family of networks.

5.1 Preliminary Theorem

Definition 3 (q-quasi-partition, see [DHMP06]) Let $G = (V, E)$ be a graph and q a positive integer. A *q-quasi-partition of G* is a family $Q = \{A_1, A_2, \ldots, A_m\}$ of subsets of V, such that :

(i) for every $1 \leq i \leq m$, the subgraph $G[A_i]$ induced by A_i is connected;

(ii) for every $1 \leq i \leq m$, $\frac{q}{2} \leq |A_i| \leq q$;

(iii) $V = \bigcup_{i=1}^{m} A_i$ and $\sum_{i=1}^{m} |A_i| \leq |V| + |\{A_i, |A_i| > \frac{2q}{3}\}|$.

Lemma 4 ([DHMP06]) *Let q be a positive integer and G be a connected graph of order at least $\frac{q}{2}$. Then G admits a q-quasi-partition.*

Remark 2

- *If G has several connected components of size at least $\frac{q}{2}$, applying the lemma to each component and using the additivity of both sides of Equation (iii) gives us a $q-$quasi-partition of G.*
- *Let Q be a quasi-partition of G as in Lemma 4. Let $t = |\{A_i, |A_i| > \frac{2q}{3}\}|$ and $v = |V|$. Then we have: $m \leq \frac{2(v+t)}{q}$ and $t \leq \frac{v}{\frac{2q}{3}-1}$.*

For the proof of Theorem 6 we need to define large and small $H-$components of $\mathcal{R}$ the associated graph of $\mathcal{N}$.

Definition 4 [H-component, large and small H-components, adjacent H-components] *We consider a (p, λ, k)-network and its associated graph $\mathcal{R}$ (cf Section 2 for definition). We take H the subgraph of $\mathcal{R}$ which contains only the edges of type E_0. An H-*component *of $\mathcal{R}$ is a connected component of H. An H-component is said* large *(respectively* small*) if it has more than (resp. strictly less than) q switches, with q the greatest integer satisfying $2(q + (2q + 2)q) + 2 \leq k - 1$. Remark that $q \sim \frac{\sqrt{k}}{2}$. Two H-components C_1 and C_2 are said* adjacent *if there exists an edge of $\mathcal{R}$ with one $R-$switch in C_1 and the other in C_2.*

Proposition 2 *(See proof in appendix)*

1. *A small H-component has no outgoing edge of kind E_2.*
2. *A small H-component has no input inside.*
3. *Two small H-components are not adjacent.*

Theorem 6 (preliminary Theorem) *In a valid network $\mathcal{N}$ with $k \leq \frac{n}{2}$, we have*

$$N(p, \lambda, k) \geq \left(\frac{3}{2}n - (k - \lambda)\right)\left(1 - \frac{7}{2\sqrt{k}} + O\left(\frac{1}{k}\right)\right) + \frac{d}{2}\left(1 + \frac{7}{2\sqrt{k}} + O\left(\frac{1}{k}\right)\right)$$

where $n = p + k$.

Proof. The complete proof is presented in appendix **??**. Here we just give an idea. Applying Lemma 4 and Remark 5.1, the union of the large H-components of $\mathcal{R}$ admits a q-quasi-partition $Q = \{A_1, \ldots, A_m\}$. So each A_j is connected and of size $\frac{q}{2} \leq |A_j| \leq q$. Using proposition 2 and the cut criterion applied to $\mathcal{B}_j$, we can prove $o(\mathcal{B}_j) < k$ (Indeed, if $o(\mathcal{B}_j) \geq k$, the cut criterion reduces to $\delta(\mathcal{B}_j) \geq k$. Furthermore A_j is connected and of size less than q, so it has at most $2q + 2$ outgoing edges and the number of small $H-$components of $\mathcal{B}_j$ is at most $2q+2$. As the size of a small $H-$component is less than q, the number of vertices in $\mathcal{B}_j$ is at most $q + (2q + 2)q$. Hence the number of outgoing edges $\delta(\mathcal{B}_j)$ is at most $2(q + (2q + 2)q) + 2$. By our choice of q it gives $k \leq \delta(\mathcal{B}_j) \leq 2(q + (2q + 2)q) + 2 \leq k - 1$ a contradiction, consequently $o(\mathcal{B}_j) < k$).

The cut criterion is now equivalent to $\delta(\mathcal{B}_j) \geq i(\mathcal{B}_j)$. Using the connectivity of $\mathcal{B}_j$ we can find an upper bound for $\delta(\mathcal{B}_j)$ in terms of different type of vertices inside $\mathcal{B}_j$. Putting all these bounds together, we obtain

$$2\sum_{j=1}^{m}|A_j| + 2m \geq 3n - d - 2(k-\lambda) \tag{4}$$

The family $\{A_j\}$ forms a quasi-partition of $\mathcal{R}$. Let $t := |\{A_j, |A_j| > \frac{2q}{3}\}|$ and v the number of vertices of $\mathcal{R}$. Then by Remark 5.1 we have $m \leq \frac{2(v+t)}{q}$ and $t \leq \frac{v}{\frac{2q}{3}-1}$ By definition of a quasi-partition: $\sum_{i=j}^{m}|A_j| \leq v + |\{A_j, |A_j| > \frac{2q}{3}\}| = v + t$.

Putting all these equations into Equation 4 gives after simplification:

$$N(p,\lambda,k) \geq \left(\frac{3}{2}n - (k-\lambda)\right)\left(1 - \frac{7}{2\sqrt{k}} + O\left(\frac{1}{k}\right)\right) + \frac{d}{2}\left(1 + \frac{7}{2\sqrt{k}} + O\left(\frac{1}{k}\right)\right)$$

□

5.2 Lower Bounds

All the proofs of the theorems of this section can be found in Appendix. Here n is $p+k$.

Theorem 7 ($\lambda = 0$) *In a valid network $\mathcal{R}$, when $k \to \infty$ with $k \leq \frac{n}{2}$, we have*

$$N(p,0,k) \geq n + \frac{n}{2} + O(\frac{n}{\sqrt{k}}).$$

In particular, we obtain a tight bound for networks with $\lambda = 0$ (see upper bound in Section 3.3).

Theorem 8 *In the simplified case, when $k \to \infty$ with $k \leq \frac{n}{2}$, we have $N(p,\lambda,k) \geq 2n + O(\frac{n}{\sqrt{k}})$.*

Theorem 9 *When $\lambda \to \infty$ and $k \to \infty$, $N(p,\lambda,k) \geq n + \frac{2}{3}n + O(\frac{n}{\sqrt{\lambda}})$.*

Theorem 10 *When $\lambda \geq 1$ and no switches of kinds V_i and V_o are allowed, when $k \to \infty$ with $k \leq \frac{n}{2}$, we have $N(p,\lambda,k) \geq n + \frac{2}{3}n + O(\frac{n}{\sqrt{k}})$.*

Theorem 11 *Let $\mathcal{N}$ be a network of N switches with the associated graph $\mathcal{R} = (V = A \cup B, E)$ such that $\mathcal{R}$ is bipartite, all vertices of A have exactly one output and all vertices of B exactly one input in the original network.*

$$N \geq n + \frac{3}{4}n + O(\frac{n}{\sqrt{k}}).$$

6 Conclusion

In this paper we propose constructions of valid $(p, \lambda, k)-$networks and give lower bounds on their size. The design problem appears to be driven by two constraints: a local one in which small patterns are forbidden and another one which is related to some global expansion property of the network. This led us to define an expansion parameter of a graph: the $\alpha-$robustness. This parameter is a generalization of the usual edge-expansion. Using graphs of $2-$robustness equal to $\Theta(\log n)$ we have constructed almost optimal simplified networks. Similarly when $k \leq \frac{n}{7}$, using graphs of large $1-$robustness we have proposed good simplified networks. Despite many answer for small values of k ($k \leq \frac{n}{7}$), little is known when k is larg.
To obtain our lower bounds, we present a powerful technique: quasi-partitioning. We think that this technique can potentially have other applications to derive lower bounds for problems of the same kind.
Some interesting open questions are:

- For a fixed α, find explicit constructions of nice α-robust graphs, graphs having large $\alpha-$robustness.

- Is there a very explicit construction as the new Zig-Zag product of [OR02] providing nice robust graphs? Does the Zig-Zag product preserve the robustness?

- What is the maximum bisection-width of a $4-$regular graph? In [MP01] it's shown that the maximal bisection width of 4-regular graphs on n vertices is at most $\frac{2n}{5}$. This shows that the $\alpha-$robustness is $< \frac{n}{2}$ for $\alpha > \frac{4}{5}$. Is it possible to obtain same results for larger values of α ensuring a maximal robustness of size at most $\frac{n}{3}$, for example?

- What is the minimum number of switches or edges in an *n-superselector* (see [Hav06, Sch06] for some constructions)?

Acknowledgment The authors would like to thank Jean-Claude Bermond, Stéphan Thomassé and Frédéric Havet for very useful and stimulating discussions as well as for reading the first drafts of this paper.

References

[AC03] N. Alon and M. Capalbo. Smaller explicit superconcentrators. *Proc. of the Fourteenth Annual ACM-SIAM SODA*, pages 340–346, 2003.

[AGM87] N. Alon, Z. Galil, and V. D. Milman. Better expanders and superconcentrators. *J. Algorithms*, 8:337–347, 1987.

[AHK99] N. Alon, P. Hamburger, and A. V. Kostochka. Regular honest graphs, isoperimetric numbers, and bisection of weighted graphs. *European Journal of Combinatorics*, 1999.

[Alo93] N. Alon. On the edge-expansion of graphs. *Combinatroics, Probability and Computing*, 11:1–10, 1993.

[AM84] N. Alon and V. D. Milman. Eigenvalues, expanders and superconcentrators. *Proc. 25th Annual Symp. on Foundations of Computer Science (FOCS), Singer Island, Florida,*, IEEE(1984):320–322, 1984.

[Bas81] L. A. Bassalygo. Asymptotically optimal switching circuits. *Problemy Pederachi Informatsii*, 17:81–88, 1981.

[BD99] B. Beauquier and E. Darrot. Arbitrary size Waksman networks. In *AlgoTel*, pages 95–100, 1999.

[BD02] B. Beauquier and E. Darrot. Arbitrary size Waksman networks and their vulnerability. *Parallel Processing Letters*, 3-4:287–296, 2002.

[BDD02] J-C. Bermond, E. Darrot, and O. Delmas. Design of fault tolerant on-boardnetworks in satellites. *Networks*, 40:202–207, 2002.

[BDH+03] J-C. Bermond, O. Delmas, F. Havet, M. Montassier, and S. Perennes. Réseaux de télécommunications minimaux embarqués tolérants aux pannes. In *Algotel*, pages 27–32, 2003.

[BGP06] J-C. Bermond, F. Giroire, and S. Pérennes. Design of minimal fault tolerant networks: Constructions. In *Submitted*, 2006.

[BHT06] J-C. Bermond, F. Havet, and D. Tóth. Fault tolerant on board networks with priorities. *Networks*, 47(1):9–25, 2006.

[BKP+81] M. Blum, R. Karp, C. Papadimitriou, O. Vornberger, and M. Yannakakis. The complexity of testing whether a graph is a superconcentrator. *Inf. Proc. Letters*, 13:164–167, 1981.

[Bol88] B. Bollobás. The isoperimetric number of random regular graphs. *European Journal of Combinatroics*, 9, no. 3:241–244, 1988.

[BPTed] J.-C. Bermond, S. Perennes, and Cs. D. Tóth. Fault tolerant on-board networks with priorities. *Manuscrit*, submitted.

[Chu79] F. R. K. Chung. On concentrators, superconcentrators, generalizers and nonblocking networks. *Bell System Tech. J.*, 58:1765–1777, 1979.

[Chu97] F. R. K. Chung. *Spectral Graph Theory*, volume No. 92. CBMS, 1997.

[CRVW02] M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson. Randomness conductors and constant-degree lossless expanders. In *STOCS*, pages 659 – 668, 2002.

[DH00] D. Z. Du and F. K. Hwang, editors. *Notes on the Complexity of Switching Networks*, volume 42. Kluwer Academic Publishers, 2000.

[DHMP06] O. Delmas, F. Havet, M. Montassier, and S. Pérennes. Design of fault tolerant on-board networks. *Research report INRIA RR 5866, submitted*, 2006.

[GKW04] C. Greenhill, J. H. Kim, and N. C. Wormald. Hamiltonian decompositions of random bipartite regular graphs. *Journal of Combinatorial Theory Series B*, no. 2, 90:195–222, 2004.

[Hav06] F. Havet. Repartitors, selectors and superselectors. *Journal of Interconnection Networks, to appear*, 2006.

[Mor94] M. Morgenstern. Existence and explicit constructions of $q+1$ regular ramanujan graphs for every prime power q. *Journal of Combinatorial Theory Series B*, 62:44–62, 1994.

[MP01] B. Monien and R. Preis. Upper bounds on bissection width of 3- and 4-regular graphs. *Mathematical foundations of computer science*, Lecture Notes in Comput. Sci., 2136, Springer, Berlin:524–536, 2001.

[Mur03] M. Murty. Ramanujan graphs. *Journal of the Ramanujan Mathematical Society*, 18:33–52, 2003.

[ND01] H. Q. Ngo and D.-Z. Du. *Notes on the complexity of switching networks*, pages 307–367. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2001.

[OR02] S. Vadhan et Z. Wigderson O. Reingold. Entropy waves, the zig-zag product and new constant-degree expanders. *Ann. of Math.(2)*, 155(1), 2002.

[Pip77] N. Pippenger. Superconcentrators. *SIAM Journal on Computing*, 6:298–304, 1977.

[Sch06] Uwe Schöning. Smaller superconcentrators of density 28. *Inform. Process. Lett. 98*, 4:127–129, 2006.

[Val75] Leslie G. Valiant. On non-linear lower bounds in computational complexity. *STOC*, pages 45–53, 1975.

A Annexe

A.1 Upper Bounds

A.2 Expanders

An expander (see [DH00] or [Mur03] for a survey) is a highly connected sparse graph. They are used in various fields of computer science and mathematics. For example in constructions of error-correcting codes with efficient encoding and decoding algorithms, derandomization of random algorithms, construction of finitely generated groups which cannot be embedded uniformly in a Hilbert space, ... but they also have applications in areas directly related to the subject of this paper as design of explicit superefficient networks and explicit construction of graphs with large girth (length of the smallest cycle). We present here known results about expanders that are used in proof of Sections 3.1, 3.2 and 3.3. The formal definition of an expander is as follows: an (n, r, c)-E-expander is a finite r-regular graph $G = (V, E)$ with n vertices such that for any set A of vertices of G with $|A| \leq |V|/2$ we have $\delta(A) \geq c|A|$. Well known examples of expanders are Ramanujan graphs (for more on Ramanujan graphs see [Mor94]). Explicit constructions of Ramanujan graphs are known for r of the form $r = q + 1$, with q a prime power (in particular for $r = 3$ and $r = 4$, which are of special interest in our case). More precisely there exist explicit constructions of an infinite family $G_i = (V_i, E_i)$ of ramanujan graphs such that $|V_i| \underset{i\to\infty}{\rightarrow} \infty$ with an expansion factor $c \geq 1 - \frac{4(r-1)}{r^2}$. It gives $c \geq \frac{1}{4}$ for $4-$regular graphs and $c \geq \frac{1}{9}$ for 3-regular graphs. The girth of the graphs of this family satisfies: $g(G_i) \geq \frac{2}{3} \log_q |V_i|$ There also exist a family $H_i = (W_i, F_i)$ of explicit *bipartite* Ramanujan graphs of girth: $g(H_i) \geq \frac{4}{3} \log_q |W_i|$. Probabilistic arguments show the existence of graphs, for *any large order of networks* (and not only for the specific values of both families), with the same properties of girth and *even better expansion factor*: for 4-regular graphs, expanders $c \geq \frac{11}{25}$ exist (see [Bol88]).

A.3 Cut Criterion for the Associated Graph

To simplify the proofs of validity of Sections 3.1, 3.2 and 3.3, it is better to work directly on the associated graph $\mathcal{R}$ of the $(p, \lambda, k)-$network $\mathcal{N} = ((V, E), i, o)$. More precisely, it means that, when applying the cut criterion on $\mathcal{N}$, it would be sufficient to consider only subsets of $\mathcal{R}$.

We introduce another notion of excess, ε', defined for all $W \subset V$ as $\varepsilon'(W) := \delta(W) + o(W) - \min(k, o(W)) - i(W)$. Note that $\varepsilon'(W) \leq \varepsilon(W)$. Hence, if, for all $W \subset V$, $\varepsilon'(W) \geq 0$, the network is valid. But we have no more an equivalence. The good property of ε' is that, if a switch D is a doublon, $\varepsilon'(W \cup \{D\}) \leq \varepsilon'(W)$. So it is enough to verify the cut criterion for subsets W of $\mathcal{N}$ consisting of a set of $R-$switches plus all the doublons on the edges of type E_1 and E_2 incident to the $R-$switches.

Definition 5 *(V-Expander) An (n, r, d)-V-expander is a finite r-regular graph $G = (V, E)$ with $|V| = n$ ($|V_1| = |V_2| = n$ in case of a bipartite graph and $V = V_1 \cup$*

V_2) such that for any subset A of vertices ($A \subset I$ when G is bipartite), the set of neighbors of $A, \Gamma(A) = \{v \in V | (v,u) \in E$ for some $u \in V\}$ satisfies

$$|\Gamma(A)| \geq |A| + d(1 - |A|/n)|A|$$

Proof. 1

Let us prove that the constructed network is valid. We use the cut criterion on $\mathcal{R}$, which is in that case exactly G. Remark first that the network is symmetric in inputs and outputs and that for any subset $W \subset V$ of vertices, $i(W) = o(W)$. Hence we have

$$\varepsilon'(W) = \delta(W) - \min(k, o(W)).$$

Furthermore, note that when a network is symmetric, it is sufficient to verify the cut criterion only for subsets W with $|W| \leq |V|/2$.

- If $|W| \geq \frac{k}{c}$ then, by the expansion property, there are at least k edges between W and $\overline{W}$ and so $\varepsilon'(W) \geq 0$.
- Otherwise, if $|W| < \frac{k}{c} \leq g$, we have $|W| < g$ and thus W is acyclic. There are at most $|W| - 1$ edges inside W and, as G is 4-regular, we have $\delta(W) \geq 2|W|+2$. Let $e_F(W)$ be the number of edges of F incident to a node of W, by construction $o(W) = e_F(W)$. As the cycles of F are disjoint, $e_F(W) \leq 2|W|$. Hence $\delta(W) \geq e_F(W) = o(W)$, that is $\varepsilon'(W) \geq 0$.

The $(p, k, k)-$network is valid. □

Proof. 1 We use the cut criterion on the associated graph following Section A.3. As the construction is symmetric in inputs and outputs, it is sufficient to consider connected subsets $W \in V$ with $|W| \leq \lceil \frac{|V|}{2} \rceil$. The cut criterion is implied by

$$\varepsilon'(W) = \delta(W) + o(W) - \min(o(W), k) - i(W) \geq 0$$

We now distinguish two cases for W.

- case 1: $|W| \leq \frac{2k}{c} \leq g$

  As $o(W) - min(o(W), k) \geq 0$, we have

  $$\varepsilon'(W) \geq \delta(W) - i(W).$$

  so it is sufficient to prove $\delta(W) \geq i(W)$ As $|W| \leq g$, there are no cycles inside W and therefore there are $|W| - 1$ edges inside; G is $3-$regular so $\delta(W) = |W| + 2$. Furthermore, $i(W) = v_1(W) + d$ so we have to prove that $v_2(W) + 2 \geq d$.

  Consider a doublon D incident to W and its associated edge $e(D) = (v_1(D), v_2(D))$ with $v_1(D) \in V_1$ and $v_2(D) \in V_2$. If $v_2(D) \in W$, associate D with $v_2(D)$. If $v_2(D) \notin W$, then $v_1(D) \in W$. Associate to D a neighboor of $v_1(D) \in W$. As the distance of two edges of $\mathcal{F}$ is at least 3, different doublons have different associate vertices in $V_2 \cap W$. So $v_2(W) \geq d$.

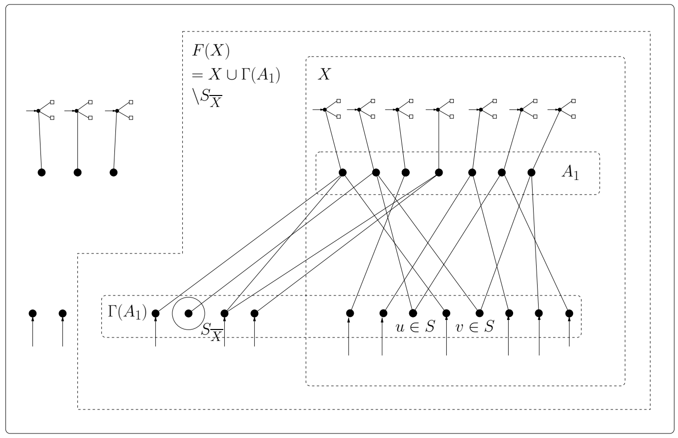

Figure 3: Sketch of proof of Theorem 3

- case 2: $|W| \geq \frac{2k}{c}$, by definition of ε' we have

$$\varepsilon' \geq \delta(W) + o(W) - k - i(W).$$

  - if $i(W) - o(W) \leq k$, by the expansion property, we have $\delta(W) \geq 2k \geq i(W) - o(W) + k$
  - if $i(W) - o(W) \geq k$, since the graph is bipartite, there is at least $3(i(W) - o(W))$ outgoing edges. So $\varepsilon'(W) \geq 2(i(W) - o(W)) - k \geq k > 0$.

$\square$

Proof. 3 To prove that this network is valid let X be a connected subset of V. Let $\overline{X} = V_1 \cup V_2 \backslash X$, $A_1 = X \cap V_1$, $S_{\overline{X}} = S \cap \Gamma(A_1) \cap \overline{X}$. We define $Z(X) = X \cup \Gamma(A_1) \backslash S_{\overline{X}}$ (Figure 3).

$Z = Z(X)$ is connected. We also have $\varepsilon(Z) \leq \varepsilon(X)$ so it is sufficient to verify the cut criterion for Z (same principles as in Section A.3). Let $A_2 = Z \cap V_2$.

We distinguish four cases for $|A_1|$:

- $|A_1| \leq \frac{k}{2}$: as $o(Z) = 2|A_1| \leq k$ and $\varepsilon(Z) \geq \delta(Z) - i(Z)$, we have $\delta(Z) \geq 3|A_2| - 3|A_1|$ and $i(Z) \leq |A_2| + |A_1|$. Furthermore there is no cycle in Z so $|A_2| \geq 2|A_1|$. Hence $\varepsilon(Z) \geq 0$.
- $\frac{k}{2} \leq |A_1| \leq \frac{k}{d} \leq \frac{g}{2}$:
we have $\varepsilon = \delta(Z) + o - i - k$ and $i \leq |A_1| + |A_2|$. So $\varepsilon(Z) \geq \delta(Z) - A_2 + A_1 - k$. As Z contains no cycle $\delta(Z) \geq 3|A_2| - 3|A_1|$ so $\varepsilon \geq 2|A_2| - 2|A_1| - k \geq 2|A_1| - k \geq 0$. We use again that $|A_2| \geq 2|A_1|$.

- $\frac{k}{d} \leq |A_1| \leq n - \frac{k}{d}$:
  in this case, $\varepsilon \geq \delta(Z) - |A_2| + |A_1| - k$ and $\delta(Z) \geq 3(|A_2| - |A_1|) = |A_2| - |A_1| + 2(|A_2| - |A_1|)$, so we have $\varepsilon \geq 2(|A_2| - |A_1|) - k$. Furthermore $|A_2| - |A_1| \geq \Gamma_G(A_1) - k$, because at most k nodes of $\Gamma_G(A_1)$ are in $S \setminus A_2$ (where $\Gamma_G(A_1)$ is the neighborhood of A_1 in G) By the expansion property we have:

  $$|\Gamma_G(A_1)| \geq |A_1| + d(1 - |A_1|/n)|A_1|$$

  In this case $d(1 - |A_1|/n) \geq 2k$. So $|\Gamma_G(A_1)| - |A_1| \geq 2k$. So $|A_2| - |A_1| \geq k$. It implies $\varepsilon \geq 0$.
- $n - \frac{k}{d} \leq |A_1|$:
  we can assume that $\overline{Z}$ is connected (see the remarks on Proposition 1). As the nodes in S are at distance at least αk and $\alpha k > \frac{k}{d}$, $\overline{Z}$ contains at most one node in S. Hence $i \geq |A_2| - k + 1 + |A_1|$ and $\varepsilon \geq \delta(Z) - |A_2| + |A_1| - 1$. Because of the connectivity of Z and the $3-$regularity $|A_2| > |A_1|$. So $\varepsilon \geq 0$.

□

A.4 Lower Bounds

Proof. 2 Let C be a small H-component. We will apply the cut criterion of Section A.3 to the set $\tilde{C}$ of $\mathcal{N}$ obtained from C by adding in $\mathcal{N}$ the doublons of the edges of type E_1 and E_2 incident to $R-$switches of C.

As $k \leq p$ and $|C| \leq q \approx \frac{\sqrt{k}}{2}$, $o(C) \leq \frac{k}{2} \leq p$ so, the cut criterion reduces to

$$\delta(\tilde{C}) \geq i(\tilde{C})$$

Let e_1 (res. e_2) be the number of outgoing edges of kind E_1 (resp. E_2) incident to $R-$switches of C.

- By definition of H and of the small components, $\delta(\tilde{C}) = e_1 + e_2$. We have $i(\tilde{C}) \geq e_1 + 2e_2 + i(C)$. So by the cut criterion $e_2 = 0$ proving 1) and $i(C) = 0$ proving 2).
- Let C' be an other small $H-$component. If C and C' are joined by $f \geq 1$ edges, then let $W = \tilde{C} \cup \tilde{C'}$, we have $i(W) \geq e_1 + e'_1 - f$ and $\delta(W) \leq e_1 + e'_1 - 2f$ so $\delta(W) < i(W)$ which gives a contradiction.

□

Proof. 7 The proof follows directly from Theorem 6 □

Proof. 8 First remark that a direct applications of the cut criterion show that as soon as $\lambda \geq 1$, T is empty. This means that in this proof and the following we will not consider switches of T. Now the proof follows from Theorem 6 and from $d = n - (k - \lambda)$ in the simplified case. □

Proof. 9 We show here that, when $\lambda \to \infty$, $N(p, \lambda, k) \geq n + \frac{2}{3}n + O(\frac{n}{\sqrt{\lambda}})$ (Theorem 9). We first give a bound for the number of switches of types V_i and V_o using the following remark:

Lemma 5 *When $\lambda \to \infty$ and $k \to \infty$,*

$$\left\{ \begin{array}{lcl} v_i & \leq & N - \frac{3}{2}n - \frac{d}{2} - \frac{k-\lambda}{2} + \lambda O(\frac{n}{\sqrt{k}}) \\ v_o & \leq & N - \frac{3}{2}(n - k + \lambda) - \frac{d}{2} + k - \frac{\lambda - k}{2} + O(\frac{n}{\sqrt{\lambda}}) \end{array} \right.$$

Proof. Imagine we have a valid $(p, \lambda, k)-$network with N switches and v_i nodes in V_i. We obtain a valid $(p, 0, k)-$network after removing any λ inputs. This new network has at least $v_i - \lambda$ switches of kind V_i. By Remark 3 we may remove these switches and obtain a valid $(p, 0, k)-$network with $N - v_i + \lambda$ switches. Theorem 6 gives

$$N - v_i + \lambda \geq \frac{3}{2}n + \frac{d}{2} + \frac{k - \lambda}{2} + O(\frac{n}{\sqrt{k}}).$$

So the result holds. Symmetry (in the sense of swapping inputs and outputs gives a valid $(p, k, \lambda)-$network) gives the second equation. □

The switch partition and the two equations **??**, **??** give here

$$N = 2n - (k - \lambda) - v_i - v_o - d + s$$

Lemma 5 gives

$$\begin{aligned} N &\geq 2n - (k - \lambda) - d + s - 2N + 3n + d \\ &\quad + O(\frac{n}{\sqrt{k}}) + O(\frac{n}{\sqrt{\lambda}}) - \frac{3}{2}(k - \lambda) - \lambda - k \\ N &\geq \frac{5}{3}n + O(\frac{n}{\sqrt{k}}) + O(\frac{n}{\sqrt{\lambda}}) - \frac{5}{2}k + \frac{\lambda}{2}. \end{aligned}$$

□

Proof. 10 We first have the following remark:

Remark 3 *Notice that when $\lambda = 0$, switches of type V_i are not present in a minimal valid $(p, \lambda, k)-$network. As shown in Figure 4, they may be removed to form a new valid $(p, \lambda, k)-$network with v_i less switches.*

Proof. Direct by the cut criterion. □

When $v_i = v_o = 0$, the input equation (Equation **??**) becomes $n = d + s_i$ and the output equation (Equation **??**) becomes $n = d + s_o$. So $s_i = s_o$ and the switch partition equation (Equation **??**) gives

$$N = 2n - d. \tag{5}$$

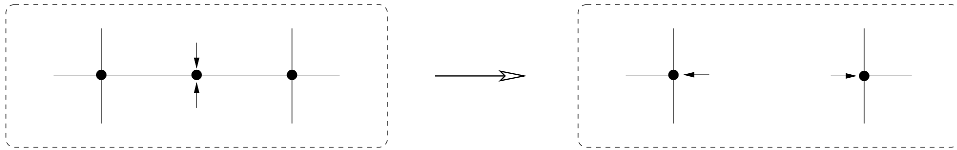

Figure 4: When $\lambda = 0$, switches of kind V_i may be removed.

Theorem 6 gives

$$2n - d \geq \frac{3}{2}n + \frac{d}{2} + O(\frac{n}{\sqrt{k}})$$
$$\frac{n}{3} \geq d + O(\frac{n}{\sqrt{k}}).$$

Equation 5 gives

$$N \geq \frac{5}{3}n + O(\frac{n}{\sqrt{k}}).$$

□

Proof. **??** We are given a ternary bipartite graph $R = (V = A \cup B, E)$ such that all vertices of A have an output and all vertices of B have an input. The vertices of B are partitioned in two sets B_1, B_0. A vertex of B_1 is adjacent to an edge of type E_1 or E_2, not those of B_0.

For subset $X \subset A$ we use the following notations : $B_i(X) = \Gamma(X) \cap B_i, i = 0, 1$ and $b_i = |B_i|$.

Let X be a subset of A such that $F(X) = X \cup \Gamma(X)$ is connected, and $6|X| \leq k$ so we have less than k outputs. To fullfill the cut-criterion for small subsets (less than k outputs), we need

$$b_0(X) \geq b_1(X) - 3 + 3c_{F(X)} \tag{6}$$

where $c_{F(X)}$ is the feed back edge set of the subgraph induced by $F(X)$.

We aim at proving that this can happen only if $b_0 + O(\frac{1}{\sqrt{k}}) \geq 2b_1$.

Let Y be a set of y vertices of B_0 such that $Y \cup \Gamma(Y)$ is connected. We have $|\Gamma(Y)| = 2y + 1 - c_{F(Y)}$ There is $3y + 3 - 3c$ edges comming out of $F(Y)$, say αy toward vertices of type B_0 and $3y + 3 - 3c - \alpha y$ toward vertices of type B_1. In G we consider the connected subgraph induced by $Z = F(Y) \cup (\Gamma(F(Y) \cap B_1)$. We have $(6-\alpha)y + 3 - 3c_{F(Y)}$ edges inside Z, so the number of vertices in $\Gamma(F(Y) \cap B_1$ is $(6-\alpha)y + 3 - 3c_{F(Y)} - y - (2y + 1 - c_{F(Y)}) - c_Z = (3-\alpha)y + 2 - 2c_{F(Y)} - c_Z$. If we take $X = \Gamma(Y)$ in Equation 6 we obtain:

$$\begin{array}{rcl} (\alpha+1)y & \geq & b_0(X) \geq b_1(X) - 3 + 3c_{F(X)} \\ & \geq & (3-\alpha)y + 2 - 2c_{F(Y)} - c_Z - 3 + 3c_{F(X)} \\ & \geq & (3-\alpha)y - 1 - 2c_{F(Y)} + 2c_{F(X)} \end{array}$$

where in the last inequality we use the fact that $c_Z \leq c_{F(X)}$ and because $c_{F(Y)} \leq c_{F(X)}$ we have:

$$\alpha \geq 1 - \frac{1}{2y}$$

We consider all the connected components of the graph induced by $B_0 \cup A$ and we take a q-quasi-partition of the big components for some q, $q = O(k)$ such that all components are of the form $F(Y)$ for some Y subset of B_0. Now we count the edges going to B_0 and B_1.

For one component D of the quasi-partition with y vertices of B_0, we find at least $(3+\alpha)y \geq 4y - \frac{1}{2}$ edges toward B_0 and at most $2y + \frac{7}{2}$ edges toward B_1 with one extremity in D.

Globally, if m is the number of components and up to some small number of recounting (Quasi-partition arguments) we get $4|A| - \frac{m}{2} = 3b_0$ edges toward B_0 and $2A + \frac{7m}{2} = 3b_1$ edges toward B_1.

Hence $b_0 \geq 2b_1 + O(\frac{1}{\sqrt{k}})$.

□

A.5 Robustness

Proof. 1 The number of ways to write a number t as the ordered sum of p non null integers is $cut(t,p) = \binom{t+p-1}{p-1}$.

Starting from the vertex 0 of the cycle, the set S can be encoded by giving two sequences of numbers : the ordered list of the lengths of the segments in S and the ordered list of the lengths of the segments in $\overline{S}$.

- If 0 belong to $\overline{S}$ then S is associated with exactly m segments on the path all having length at least 1, and $\overline{S}$ is associated to $m+1$ segments, all the segments of $\overline{S}$ but the last one have all length at least 1 and the last segment can have length 0.

  So $\overline{S}$ can be encoded by dividing $|\overline{S}| - m = n - s - m$ into $m+1$ non null numbers. There is exactly $cut(n-s-m, m+1)$ way of doing it.

  We write S as the ordered sum of m non null numbers, there is $cut(s-m, m) = \binom{s-1}{m-1}$ possibilities.

  This gives: $cut(n-s-m, m+1) \cdot cut(s-m, m) = \binom{s-1}{m-1}\binom{n-s}{m}$

- If 0 is in S, then the situation is symmetric, so we only need to change s by $n-s$, i.e. we replace $cut(n-s-m, m+1)cut(s-m, m)$ by $cut(s-m, m+1)cut(n-s-m, m) = \binom{s}{m}\binom{n-s-1}{m-1}$.

□

Proof. 2 Consider a bipartite graph whose vertices are the sets of s elements and the $(n-1)!$ cyclic permutations. We put an edge between a set and a cyclic permutation if the set defines m segments on the cycle associated to the permutation. This graph is a "regular bipartite graph", where sets have degree Δ and the permutations degree is $I(s,m)$. Counting the edges of the graph we get $\Delta = \frac{(n-1)!I(s,m)}{\binom{n}{s}}$.

Now, the probability for a set to be adjacent to a permutation is $\Delta/(n-1)!$. So given a set S with s elements, the probability that S defines exactly m segments on a cycle C is $I(s,m)/\binom{n}{s}$. Then lemma 1 gives the result. □

Proof. 3 The result follows from those three points :

- the probability S defines k_i segments on a random cycle C_i is $I(s,k_i)$
- the cycles constituting $G(n,m)$ are independents
- $|\Gamma(S)| = 2\sum_{1,2,\ldots m} k_i$.

□

Proof. 2

Let $W(n,s)$ be the probability there is a set of size $s \leq r$ with border less than s, $W(n,s) \leq \binom{n}{s} \sum_{r\leq s/2} \sum_{m_1+m_2=r} I(s,m_1)I(s,m_2)/\binom{n}{s}^2$.

Since $I(s,m_1)I(s,m_2) \leq I(s,\frac{m_1+m_2}{2})$, we have

$$W(n,s) = \sum_{r\leq s/2} \sum_{m_1+m_2=r} I(s,m_1)I(s,m_2)/\binom{n}{s} \leq \sum_{r\leq s/2} r(I(s,r/2))^2/\binom{n}{s}$$

.

Now since $r \leq s/2$, we have $I(s,r/2) \leq I(s,s/4)$ and $W(n,s) \leq \frac{s^2}{8}\left(I(s,s/4)\right)^2/\binom{n}{s}$.

Replacing $I(s,s/4)$ by its value we get:

$$W(n,s) \leq \frac{s^2}{8} \binom{s}{s/4}^2 \binom{n-s}{s/4}^2 / \binom{n}{s}$$

For the following we need the following rather sharp form of *Stirling's formula* proved by Robbins(1955):

$$n! = \left(\frac{n}{e}\right)^n \sqrt{2\pi n} e^{\alpha_n}$$

where $\frac{1}{12n+1} < \alpha_n < \frac{1}{12n}$

Putting this formula in the above inequality we obtain:

$$W(n,s) \leq \frac{s^{3s}(n-s)^{3n-3s}}{(\frac{s}{4})^s(\frac{3s}{4})^{\frac{3s}{2}}(n-\frac{5s}{4})^{2n-\frac{5s}{2}}\ n^n}\ \beta$$

Where $\beta = \frac{16\ (n-s)\sqrt{s(n-s)}}{3\pi\sqrt{2\pi n}\ (4n-5s)}.e^{\gamma}$ and

$$\gamma = 3\alpha_s + 3\alpha_{n-s} - 4\alpha_{\frac{s}{4}} - 2\alpha_{\frac{3s}{4}} - 2\alpha_{n-\frac{5s}{4}} - \alpha_n$$

and α_i is a real number in the interval $[\frac{1}{12i+1}, \frac{1}{12i}]$. Let

$$X(n,s) = \frac{s^{3s}(n-s)^{3n-3s}}{(\frac{s}{4})^s(\frac{3s}{4})^{\frac{3s}{2}}(n-\frac{5s}{4})^{2n-\frac{5s}{2}}\ n^n}\ \beta$$

Suppose $n = a \cdot s$ then we have:

$$X(n,s) = \left(\frac{(a-1)^{3(a-1)}}{\frac{1}{4}.(\frac{3}{4})^{\frac{3}{2}}.(a-\frac{5}{4})^{2a-\frac{5}{2}}.a^a}\right)^s \beta$$

Let

$$g(a) = \frac{(a-1)^{3(a-1)}}{\frac{1}{4}.(\frac{3}{4})^{\frac{3}{2}}.(a-\frac{5}{4})^{2a-\frac{5}{2}}.a^a}$$

then we have:

$$X(n,s) = g(a)^s.\beta$$

Remember that

$$\beta = \frac{16\ (n-s)\sqrt{s(n-s)}}{3\pi\sqrt{2\pi n}\ (4n-5s)}.e^\gamma$$

It's now easy to see that g is decreasing and $g(13.80\dots)$ so $g(14) < 1$ and we have

- for $s \in [-\frac{4\log n}{\log(g(14))}, \frac{n}{14}]$ we have

  $$X(n,s) \leq C.\frac{1}{n^4}\beta = O(\frac{1}{n^2}).$$

  and so

  $$W(n,s) \leq C.\frac{1}{n^2}$$

  for some constant C.

- for $s \leq -\frac{4\log n}{\log(g(14))}$ we have $a \geq C.\frac{n}{\log n}$ for some constant C. Then we have

  $$X(n,s) \leq C.(n/s)^{-\frac{s}{2}}.\beta$$

  For some constant C. It's clear then that for $s \geq 4$, we have: $X(n,s) \leq C.\frac{1}{n}$ for some constant C.

- It's easy to show that $W(n,s) = 0$ for $s = 1, 2, 3$ because the graph connectivity is 4 with probability 1.

Then we have

$$\sum_{s\leq \frac{n}{14}} W(n,s) \leq \sum_{-\frac{4\log n}{\log(g(14))}\leq s\leq \frac{n}{14}} X(n,s) + \sum_{s\leq -\frac{4\log n}{\log(g(14))}} X(n,s) < C.n.\frac{1}{n^2} + C.\log(n).\frac{1}{n} < \frac{1}{2}.$$

for n large enough. □

Proof. 3

A set larger than $\frac{n}{14}$ is bad when its border is smaller than $\frac{n}{14}$.

Let first $W'(n,s)$ be the probability that there exists a set with size $s \geq r$ with border less than r, $W'(n,s) \leq \sum_{i\leq \frac{n}{28}} \sum_{k_1+k_2=i} I(s,k_1)I(s,k_2)/\binom{n}{s}$. and so $W'(n,s) \leq \frac{(\frac{n}{14})^2}{8}\left(I(s,\frac{n}{56})\right)^2/\binom{n}{s}$.

Let for $a \in [\frac{1}{14}, 1-\frac{1}{14}]$

$$\delta(a) = \frac{\left(\binom{a.n}{\frac{n}{56}}\binom{(1-a)n}{\frac{n}{56}}\right)^2}{\binom{n}{a.n}}$$

Then

$$W'(n,an) \leq \frac{1}{8}(\frac{n}{14})^2\delta(a)$$

Again using the same methods than the one we used in the last section we obtain $W'(n,a) \leq h(a)^n\beta'$ where β' is a rational function on n and a and h defined below:

$$h(a) = \frac{a^{3a}\ (1-a)^{3-3a}}{(\frac{1}{56})^{\frac{1}{14}}\ (a-\frac{1}{56})^{2a-\frac{1}{28}}\ (1-a-\frac{1}{56})^{2-2a-\frac{1}{28}}}\beta'$$

Since $h(\frac{1}{14}) < 1$, with h decreasing

$$W'(n,an) \leq h(\frac{1}{14})^n\beta'$$

As β' is rational we have for n large enough $W'(n,an) < \frac{1}{2n}$ so

$$\sum_{s\in[\frac{n}{14}\ ,\ \frac{13n}{14}]} W'(n,s) < \frac{1}{2}$$

and the lemma is proved. □

Proof. 5 Suppose given a 4−regular Hamiltonian graph G of robustness $\frac{n}{7}$ on $2n$ vertices. Extract a complete matching from a Hamiltonian cycle and add a doublon to every edge of this matching. It's now straightforward to show that the resulting network is valid. This gives a valid $(p = n-k, k, k)$-network on $3n$ nodes. □