EXPECTED RELIABILITY OF COMMUNICATION PROTOCOLS

ANDRÉ KÜNDGEN AND JANINA PATNO

Abstract. We consider the problem of sending a message from a sender $s$ to a receiver $r$ through an unreliable network by specifying in a protocol what each vertex is supposed to do if it receives the message from one of its neighbors. A protocol for routing a message in such a graph is finite if it never floods $r$ with an infinite number of copies of the message. The expected reliability of a given protocol is the probability that a message sent from $s$ reaches $r$ when the edges of the network fail independently with probability $1 - p$.

We discuss, for given networks, the properties of finite protocols with maximum expected reliability in the case when $p$ is close to 0 or 1, and we describe networks for which no one protocol is optimal for all values of $p$. In general, finding an optimal protocol for a given network and fixed probability is challenging and many open problems remain.

1. Introduction

All graphs $G$ in this paper will be undirected, simple (no loops or multiple edges), and have two distinct vertices identified as $s$ (the sender) and $r$ (the receiver). Our goal is to pass a message from $s$ to $r$ along the edges of $G$, where we will assume that edges may fail, but vertices do not. We will also assume that vertices are memoryless and have no information about which edges have failed and which are alive, but rather, will pass the message along based on a set of instructions that are given before we know which edges fail. More formally, an instruction is any triple $uvw$ where $u, w$ are different neighbors of $v$ and the idea is that if $v$ receives a message from $u$, then it passes it on to $w$. (We require that $u \neq w$, since there is no point in sending a message back where it came from. Also observe that $uvw$ and $wvu$ are different instructions, whereas for edges we have $uv = vu$ as usual.) A protocol $A$ is a set of instructions. For a protocol $A$ of a graph $G$ we now try to send a message from $s$ to $r$ by sending one copy of the message from $s$ to everyone of its neighbors, and whenever an intermediate vertex receives the message, it passes it on as described by $A$.

There are several considerations of what makes a good protocol. A very basic one is that we do not want to flood the receiver, that is, we do not want $r$ to receive infinitely
many copies of the message. This is what would usually happen if no edge fails and every intermediate vertex simply sends the message to every neighbor each time it receives it. This basic consideration is studied in [3]. Another consideration is that we would like our protocol to have a certain robustness, that is the failure of only few edges does not interrupt communication. This concept was suggested to the first author by Lovász and is studied in [6]. A second approach suggested by Lovász [6] is to study the probability that a message sent from s will reach r when the edges of G only survive with some probability p. This approach was first studied in the Master’s thesis of the second author [8]. In this paper we build on the ideas from [3, 6, 8] to investigate the probabilistic setting.

2. The basic model

To study this communication model we need a few basic definitions that are consistent with those used in [3, 6, 8, 10]. A u, v-walk of length k in a graph G is a sequence v_0, v_1, v_2, ..., v_k-1, v_k of vertices such that v_0 = u, v_k = v and v_i, v_i-1 are adjacent for all i with 1 ≤ i ≤ k. We say that an instruction uvw is contained in this walk if there is an index i such that u = v_{i-1}, v = v_i, w = v_{i+1}. A trail is a walk such that if v_i = v_j for i ≠ j, then v_{i+1} ≠ v_{j+1}. Thus, each edge uv can be used at most twice in a trail: once as u, v and once as v, u. (This is a slightly nonstandard use of this term.) A walk (trail) is closed if the endpoints, v_0 and v_k, of the walk (trail) are the same. A path is a walk v_0, v_1, v_2, ..., v_k-1, v_k such that v_0, v_1, ..., v_k-1, v_k are distinct vertices of G. For a protocol A, an A-walk is an s, r-walk such that every instruction it contains is in A. The concepts of A-trail and A-path are defined similarly.

Using this notation it is now easy to see that r receives the message exactly once for every A-walk whose edges do not fail. To have a good protocol we generally want there to be many A-walks, but we also do not want to flood the receiver with infinitely many messages when no edge fails. Thus we call a protocol A finite if there are only finitely many A-walks. To characterize such protocols we call an instruction (strongly) essential for A if it is contained in an A-walk (an A-path). If every instruction of A is (strongly) essential, then we call A a (strongly) essential protocol. One of the key lemmas of [3] is that a protocol A is finite if and only if it does not contain an essential circuit, that is a closed trail such that every instruction it contains (including v_k-1v_kv_1) is essential for A.

The simplest protocol is the Complete Forwarding Protocol (CFP) A* = \{uvw : uvw is contained in some s, r-path\}. By definition A* is strongly essential. Observe that there can be instructions that are contained in an s, r-walk, but not in an s, r-path and such instructions would not be in A*.

\textbf{Example 1.} The graph B_0 in Figure 1 has Complete Forwarding Protocol A* = \{s13, s14, s23, s25, 132, 134, 135, 143, 14r, 231, 234, 235, 253, 25r, 314, 325, 34r, 35r, 432, 435, 531, 534\}.
Observe that 413 ∉ A*, even though there is an s, r-walk s, 2, 3, 4, 1, 3, 5, r. Every essential circuit must contain the edges of a cycle, but not s or r. It is easy to see that C = 1, 4, 3, 2, 5, 3, 1 is the only essential circuit of A* up to the choice of the starting point.

The graph B₀ shows that the CFP need not be finite. In fact the main result of [3] is a characterization of the graphs for which the CFP is finite in terms of 10 forbidden minors, one of which is B₀. Any protocol A with A ⊆ A* is called a Partial Forwarding Protocol (PFP). An SPFP is a strongly essential PFP, that is a protocol A in which every instruction is contained in an A-path. Our first lemma will imply that in general it suffices to study SPFP’s.

**Lemma 1.** If A is a protocol for a graph G, then there is a PFP A’ with the following properties:

(a) The edge-set of every A-walk contains an A’-path.
(b) The edge-set of every A’-walk contains an A’-path.
(c) Every instruction in A’ is contained in an A’-path (and thus strongly essential).
(d) If A is finite, then A’ is finite.

**Proof.** Observe that every A-walk W = v₀, v₁, . . . , vₖ contains an s, r-path P = u₀, . . . , uₘ such that for every uᵢ we can find indices j ≤ j’ with vⱼ = uᵢ = vⱼ’, uᵢ₋₁ = vⱼ₋₁ and uᵢ₊₁ = vⱼ₊₁. Moreover, there are only finitely many s, r-paths in G, so we can let the paths obtained in this way be P₁, . . . , Pₖ, and Wᵢ be some A-walk that contains Pᵢ in this way. Let A’ = {uvw : uvw is contained in some Pᵢ}. A’ is a PFP, and since every Pᵢ is an A’-path, (a) and (c) clearly hold.

To prove (d), suppose A’ is not finite and there is an essential circuit C’ = (u₀, u₁, . . . , uₖ) for A’. Every instruction uᵢ₋₁uᵢuᵢ₊₁ in this circuit must be contained in some Pᵢ. Now by construction the A-walk Wᵢ contains a subwalk vⱼ₋₁, vⱼ, . . . , vⱼ’, vⱼ₊₁ that includes only instructions that are essential for A, and such that uᵢ = vⱼ = vⱼ’, uᵢ₋₁ = vⱼ₋₁ and uᵢ₊₁ = vⱼ₊₁. Thus if in C’ we replace every vertex uᵢ by the corresponding walk vⱼ, . . . , vⱼ’, then we obtain an essential circuit C for A. Thus A is not finite.

To prove (b) consider A” obtained from A’ by repeating the same procedure, that is A” = (A’)’. By (c) for A’ it follows that A’ ⊆ A”, so that every A’-path is an A”-path. Thus (a) holds for A” instead of A’, and (c) and (d) follow similarly with A” instead of A’. If A’ does not satisfy (b), then we get that one of the paths Pᵢ in the construction of A” from A’
is not an \( A' \)-path, so that \( A'' \) has an instruction that is not in \( A' \), that is \( A' \subset A'' \). Repeating this procedure we get a strictly increasing sequence \( A' \subset A'' \subset A''' \subset \ldots \) of protocols that satisfy (a,c,d). Since there are only finitely many instructions, this process terminates in a protocol satisfying all four conditions, which will be our \( A' \).

3. The probabilistic model

Suppose every edge of \( G \) fails with probability \( 1 - p \) and survives with probability \( p \), where \( p \) is usually fixed in \((0,1)\), but for the purpose of this section \( p \) need not be constant on \( E(G) \).

We define the (expected) reliability of a protocol \( A \) for \((G,p)\), denoted by \( \rho_A(G,p) \) or simply \( \rho_A \) if \( G \) and \( p \) are clear from the context, to be the probability that a message sent from \( s \) under protocol \( A \) reaches \( r \). Note that this is defined, whether \( A \) is finite or not. More formally

**Definition 1.** Let \( A \) be any protocol for \( G \), and \( p : E(G) \to (0,1) \). Then \( \rho_A(G,p) \) and \( \rho_A'(G,p) \) are the probability that the edges of some \( A \)-walk (respectively \( A \)-path) do not fail if every edge \( e \in E(G) \) fails independently with probability \( 1 - p(e) \). Moreover, \( \hat{\rho}(G,p) = \max\{\rho_A(G,p) : A \text{ is finite}\} \).

Note that \( \rho_A'(G,p) \leq \rho_A(G,p) \) and the former is usually easier to determine, but equality need not hold. Observe also that \( \hat{\rho} \) is well-defined since there are only finitely many protocols \( A \), but that for different choices of \( p \) this maximum might be achieved for different protocols \( A \). Also note that the well studied (two terminal)-reliability \( \rho(G,p) \) (see [2, 4, 5, 7, 9, 11]) is the probability that \( s, r \) are in the same component of \((G,p)\). This is identical to the probability that some \( s, r \)-path survives in \((G,p)\), that is \( \rho(G,p) = \rho_A(G,p) = \rho_A'(G,p) \).

Lemma 1 immediately implies the following.

**Proposition 1.** For every protocol \( A \) there is a SPFP \( A' \) such that \( \rho_A(G,p) \leq \rho_A'(G,p) = \rho_A'(G,p) \) for every \( p : E(G) \to (0,1) \). \( \rho_A(G,p) = \rho_A'(G,p) \) if and only if every \( A' \)-path is an \( A \)-path. Moreover if \( A \) is finite, then \( A' \) is finite.

**Proof.** For given \( A \) let \( A' \) be as in Lemma 1. By (c) \( A' \) is an SPFP and by (d) \( A' \) is finite when \( A \) is finite. Now if we let \( Y_i \) be the event that the edges of the \( A' \)-path \( P_i \) survive, \( X \) be the event that an \( A \)-walk from \( s \) to \( r \) survives, and \( Z \) be the event that an \( A' \)-walk from \( s \) to \( r \) survives, then \( X \subseteq Y_1 \cup Y_2 \cup \ldots Y_k \subseteq Z \) by (a) and the fact that every \( A' \)-path is an \( A' \)-walk. Moreover the second containment is equality by (b). Thus \( \rho_A(G,p) = \Prob(X) \leq \Prob(Y_1 \cup \ldots \cup Y_k) = \rho_A'(G,p) = \Prob(Z) = \rho_A(G,p) \), as desired.

If every \( A' \)-path is an \( A \)-path, then \( \rho_A' \leq \rho_A \). Since every \( A \)-path is an \( A \)-walk, it now follows that \( \rho_A \leq \rho_A \leq \rho_A' \leq \rho_A' \) and the desired equality holds. Now suppose that some \( A' \)-path \( P_i \) is not an \( A \)-path. Let \( Y \) be the event that only the edges in \( P_i \) survive, but all other edges fail. Clearly \( Y \subseteq Y_i \) and \( \Prob(Y) > 0 \) since every edge \( e \) has \( 0 < p(e) < 1 \). Moreover, \( E(P_i) \) does not contain an \( A \)-walk, since otherwise we would get the contradiction.
that either $P_i$ is an $A$-path, or that the $A$-walk contains an instruction of the form $uvu$. Thus $X \subseteq (Y_1 \cup \cdots \cup Y_k) - Y$, and we get that $\rho_A < \rho'_{A'}$. \hfill \Box$

**Definition 2.** We call a finite SPFP $A$ optimal for $(G, p)$ if for every finite protocol $A'$ we have $\rho_{A'}(G, p) \leq \rho_A(G, p)$, and $\rho_A(G, p)$ is the probability that some $A$-path survives.

Proposition 1 immediately implies that for every $(G, p)$ there is an optimal SPFP $A$ and

$$\hat{\rho}(G, p) = \max\{\rho'_{A'}(G, p) : A \text{ is a finite SPFP}\}.$$  

For an (optimal) SPFP $A$ we can compute $\rho_A(G, p) = \text{Prob}(Y_1 \cup \cdots \cup Y_k)$ by Inclusion-Exclusion once we know all $A$-paths $P_i$. Thus $\rho_A(G, p)$ is a polynomial in $p$ if $p$ is constant. Moreover, since there are only finitely PFP’s it follows that $\hat{\rho}(G, p)$ is piecewise polynomial in $p$ if every edge has the same probability $p$.

4. Series-parallel replacements

In this section we present a method for building large graphs whose reliability can be computed easily.

Given graphs $G_1$, $G_2$ with senders $s_1, s_2$ and receivers $r_1, r_2$ respectively, we can obtain a graph $H$ with sender $s$ and receiver $r$ by series operation, written $H = G_1 \circ G_2$, by setting $s = s_1$, $r = r_2$, and identifying $r_1, s_2$ with a new vertex $x$. We obtain $H$ by parallel operation, written $G_1||G_2$, by identifying $s = s_1 = s_2$ and $r = r_1 = r_2$. Any graph that can be built from $K_2$ using only these operations is called series-parallel.

**Proposition 2.** Let $H$ be a series-parallel graph, $A_{s,r}$ the CFP in $H$ and $A_{s,r}$ be the CFP in $H$ if we interchange $s$ and $r$. If $A_H \subseteq A_{s,r} \cup A_{r,s}$, then every walk $W = v_0, v_1, \ldots, v_k$ such that $v_{i-1}v_iv_{i+1} \in A_H$ for all $i$ with $1 \leq i \leq k - 1$ is a path. Specifically if $W$ is nontrivial, then it is not closed.

**Proof.** The first statement immediately implies the second, and so it suffices to prove the former.

Using the recursive definition of $H$ it is easy to show that there is an injection $f : V(H) \to [0, 1]$ such that $f$ is increasing along every $s, r$-path. Thus $f$ is strictly increasing along every instruction in $A_{s,r}$, and strictly decreasing along every instruction in $A_{r,s}$. Suppose $W$ is such a walk. Since $H$ has no loops we may assume that $k \geq 2$ and $f(v_0) \neq f(v_1)$. If $f(v_0) < f(v_1)$, then it follows that $v_0v_1v_2 \in A_{s,r}$ and thus $f(v_1) < f(v_2)$. Continuing along it follows that $f$ is strictly increasing along $W$ and thus all $v_i$ must be distinct. If $f(v_0) > f(v_1)$, then it follows similarly that $f$ is strictly decreasing along $W$. \hfill \Box

Proposition 2 implies that the CFP $A^*$ for a series-parallel graph $H$ is finite (as it has no essential circuit), and thus $\hat{\rho}(H) = \rho(H)$. Moreover, it is easy to compute $\rho(H)$ when $H$ is series parallel, since in general $\rho(G_1 \circ G_2) = \rho(G_1)\rho(G_2)$ and $\rho(G_1||G_2) = \rho(G_1) +$
\[ \rho(G_2) - \rho(G_1) \rho(G_2). \]

Our next result generalizes these equations and exploits the fact that \( p : E(G) \to (0,1) \) need not be constant.

**Definition 3.** Let \( G_1, H \) be graphs with specified vertices \( s, r \). If \( e_1 = xy \) is an edge in \( G_1 \), then let the \( G \) be the graph obtained from \( G_1 - e_1 \) by identifying \( s, r \) in \( H \) with \( x, y \) in \( G_1 \). (See Figure 2 for an example.) We call \( G \) the expansion of \( G_1 \) at \( e_1 \) by \( H \). If \( p \) is a probability distribution on \( E(G) \), then the implied distribution \( p_1 \) on \( G_1 \) is given by \( p_1(e) = p(e) \) for \( e \neq e_1 \), and \( p_1(e_1) = \rho(H, p|_H) \), where \( p|_H \) is the restriction of \( p \) to \( E(H) \).

If \( uvw \) is an instruction in \( G_1 \), then the corresponding set of instructions \( I(uvw) \) in \( G \) is given by \( I(uvw) = \{uvw\} \) (when \( e_1 \neq uw, vw \)), \( I(uvw) = \{u'vw : u' \in N_H(v)\} \) (when \( e_1 = uv \)) and \( I(uvw) = \{uvw' : w' \in N_H(v)\} \) (when \( e_1 = vw \)) where \( N_H(v) \) denotes the set of neighbors of \( v \) in \( H \). If \( A \) is a set of instructions in \( G_1 \), then we let \( I(A) = \bigcup_{uvw \in A} I(uvw) \).

Let \( A_{u,v} \) denote the CFP on \( H \) with \( s = u, r = v \) and let \( A \) be any protocol for \( G_1 \). If there are some \( A \)-paths in \( G_1 \) containing \( xy \) in which \( x \) directly precedes \( y \) and some in which \( y \) directly precedes \( x \), then we define \( A_H = A_{x,y} \cup A_{y,x} \). If no \( A \)-path in \( G_1 \) contains \( xy \) we let \( A_H = \emptyset \). If in every \( A \)-path in \( G_1 \) that contains \( xy \) we have that \( x \) immediately precedes \( y \) ( \( y \) immediately precedes \( x \) ), then we let \( A_H = A_{x,y} \) and \( A_H = A_{y,x} \) respectively. In any case \( A_H \) satisfies the hypothesis of Proposition 2 when \( H \) is series-parallel. With this notation we will define the extension of \( A \) to \( G \) by \( A^+ = I(A) \cup A_H \).

![Figure 2. G obtained from B0 by replacing s1, s2 by H1, H2](image)

**Proposition 3.** Let \( H \) be a series-parallel graph, and \( G \) be the expansion of some graph \( G_1 \) at some edge \( e_1 = xy \) by \( H \). If \( (G, p) \) is a given probability distribution and \( p_1 \) is its implied distribution on \( G_1 \), then the following hold:

(a) For every protocol \( A \) for \( G_1 \): \( \rho'_A(G_1, p_1) = \rho'_A(G, p) \).

(b) \( \rho(G, p) = \rho(G_1, p_1) \).

(c) If \( A, A' \) are protocols for \( G_1 \), then \( A^+ \subseteq (A')^+ \) iff \( A \subseteq A' \).

(d) For every protocol \( A \) for \( G_1 \): \( A \) is a finite SPFP for \( G_1 \) if and only if \( A^+ \) is a finite SPFP for \( G \).

(e) \( \hat{\rho}(G, p) \geq \hat{\rho}(G_1, p_1) \) with equality if \( e_1 \) is in no essential circuit for the CFP of \( G_1 \).

**Proof.** Let \( T_{u,v} \) be the set of \( u,v \)-paths in \( H \). For every path \( P = v_0, \ldots, v_k \) in \( G_1 \) let \( P^+ \) be the following family of paths in \( G \): If \( e_1 = xy \) is not on \( P \), then \( P^+ = \{P\} \). If \( v_1 =
Let $A$ be any protocol for $G_1$. If $P$ is an $A$-path, then it follows that $P^+$ is a family of $A^+$-paths. Similarly if some member of $P^+$ is an $A^+$-path, then $P$ is an $A$-path. So the sets $P^+$ form a partition of the family of $A^+$-paths. If $X_i$ is the event that all edges of the $A$-path $P_i$ survive in $(G_1, p_i)$ and $Y_i$ is the event that the edges of some path in $P_i^+$ survive in $(G, p)$, then it is not hard to see that for every collection of indices $J$, $\Pr(G_1, p_i) (\cap_{i \in J} X_i) = \Pr(G, p) (\cap_{i \in J} Y_i)$. Thus by inclusion-exclusion it follows that (a) holds:

$$\rho'_{A_1}(G_1, p_1) = \Pr(G_1, p_1)(X_1 \cup X_2 \cup \cdots \cup X_k) = \Pr(G, p)(Y_1 \cup Y_2 \cup \cdots \cup Y_k) = \rho'_{A^+}(G, p).$$

Let $A_1^*$ be the CFP on $G_1$ and $A^*$ be the CFP on $G$. Since every $s, r$-path in $G$ is in $P^+$ for some $s, r$-path $P$ in $G_1$, it follows that $A^* = (A_1^*)^+$. Thus $\rho(G_1, p_1) = \rho'_{A_1^*}(G_1, p_1) = \rho'_{A^+}(G, p)$, and (b) holds.

If $A \subseteq A'$, then $I(A) \subseteq I(A')$ and $A_H \subseteq A'_H$, so that $A^+ \subseteq (A')^+$. If $A^+ \subseteq (A')^+$, then $I(A) \subseteq I(A')$ and thus $A \subseteq A'$, so that (c) follows.

$A$ is a PFP for $G_1$ iff $A^+$ is a PFP for $G$ follows by combining (c) and $A^* = (A_1^*)^+$. Let $uvw \in A$. Then $uvw$ is strongly essential for $A$ iff $uvw$ is contained in some $A$-path $P$ iff every $xyz \in I(uvw)$ is contained in some member of $P^+$ for some $A$-path $P$ iff every $xyz \in I(uvw)$ is in an $A^+$-path iff every $xyz \in I(uvw)$ is strongly essential for $A^+$. Furthermore every element of $A_H$ is trivially strongly essential for $A^+$ by definition. Thus $A$ is an SPFP iff $A^+$ is an SPFP.

It remains to consider finiteness, where we may now assume that every instruction in $A$ and $A^+$ is essential. Replacing every occurrence of the edge $e_1$ in an essential circuit for $A$ in $G_1$ with a path from $T_{x,y}$ or $T_{y,x}$ as appropriate it is easy to see that we obtain an essential circuit for $A^+$ in $G$. So suppose $G$ contains an essential circuit $C$ for $A^+$. Then Proposition 2 implies that $C$ cannot be entirely contained in $H$ (and thus only contain instructions from $A_H$), and that if $C$ enters $H$ at one of $x, y$, then it must leave it at the other. Thus if we remove all vertices in $V(H) - \{x, y\}$ from the sequence $C$, then we get a closed walk $C'$ in $G_1$. Moreover, by construction of $A^+$ it follows that every instruction $uvw$ contained in $C'$ is in $A$, so that $C'$ must be an essential circuit in $G_1$ and (d) is proven.

For (e) it follows so far that

$$\hat{\rho}(G_1, p_1) = \max\{\rho'_{A_1}(G_1, p_1) : A \text{ is a finite SPFP for } G_1\} = \max\{\rho'_{A^+}(G, p) : A \text{ is a finite SPFP for } G_1\} = \max\{\rho'_{A^+}(G, p) : A^+ \text{ is a finite SPFP for } G\} \leq \max\{\rho'_{B}(G, p) : B \text{ is a finite SPFP for } G\} = \hat{\rho}(G, p).$$

For equality it remains to show that for every finite SPFP $B$ for $(G, p)$ there is a finite SPFP $A$ for $(G_1, p_1)$ with $\rho'_{B}(G_1, p_1) \leq \rho'_{A^+}(G, p)$. For a given $B$, consider $A = \{uvw \in A_1^* :
I(uvw) ∩ B ≠ ∅}. We first show that B ⊆ A⁺, since then ρ_B⁺(G, p) ≤ ρ_A⁺(G, p) is trivial. So let abc ∈ B be given. Since B is an SPFP there is a B-path Q containing abc. For this path Q in G there must be a path P in G₁ with Q ∈ P⁺. Now for every instruction uww contained in P we have that I(uww) has an instruction in Q and thus B. Hence P is an A-path, and thus Q ∈ P⁺ is an A⁺-path. Specifically abc ∈ A⁺, as desired.

It remains to show that A is a finite SPFP. A is a PFP since A ⊆ A⁺. If uww ∈ A, then there is abc ∈ B with abc ∈ I(uww). As in the previous argument, abc is in some B-path Q, and there is an A-path P with Q ∈ P⁺. Since abc is in Q and I(uww) we have that uww is an instruction in (the A-path) P. Thus A is an SPFP. Finally, suppose that A is not finite, that is it contains an essential circuit C = v₀, . . . , vₖ in G₁. Since by assumption C does not use e₁ then every instruction in A is also in B, so that C is an essential circuit in B, a contradiction. □

5. Discrepancies

In general we are more interested in finding an optimal protocol for (G, p), than the actual value of ̂ρ(G, p). Since ̂ρ can be very close to ρ it makes sense to study the difference between these parameters.

**Definition 4.** Let A* be the CFP on G. For a set of instructions I ⊆ A*, we define its discrepancy d_I as d_I = d_I(G, p) = ρ(G, p) − ρ_{A*−I}(G, p). The minimum discrepancy ̂d of G is defined as ̂d = ̂d(G, p) = ρ(G, p) − ̂ρ(G, p) = min{d_I(G, p) : A* − I is finite}.

Thus d_I is the probability that some s, r-walk remains, but that every such s, r-path contains an instruction in I. Observe that if I₁ ⊆ I₂, then it follows directly that d_I₁ ≤ d_I₂, that is d_I is monotone in I. The following result is easy to see, but a proof is Lemma 3.3.5 of [8] with the notation for d_I being d_{A*−I}.

**Lemma 2.** Let (G, p) and I ⊆ A*. If P₁, . . . , P_k are the s, r-paths that use at least one instruction from I, and Z_i is the event that the edges in P_i all survive, but every s, r-trail not using an instruction from I has a failed edge, then d_I = Prob(Z₁ ∪ · · · ∪ Z_k).

The following example will give an indication on how the minimum discrepancy of a graph can be determined, and we will use this result in the proof of Theorem [3]. The discrepancies of all 10 forbidden minors for A* to be finite are computed in Chapter 4 of [8] for the case when p is constant on E(G).

**Example 2.** Let B₀ be the graph from Example [1] and let p, p₁, p₂ ∈ (0, 1). Let p’ be the probability distribution on E(B₀) given by assigning probability p to every edge, except that s₁ receives probability p₁ and s₂ receives probability p₂. Let P = s, 1, 4, 3, 2, 5, r and P’ = s, 2, 5, 3, 1, 4, r. Let X be the event that the 6 edges in P survive and all others fail. Define X’ for P’ similarly.
To find the minimum discrepancy $\hat{d}$ of $(B_0, p')$, consider the instruction 432. Observe that $A^* - 432$ is finite, since this instruction is used in the only essential circuit $C$. The only $s, r$-path using 432 is $P_1 = P$. With the notation from Lemma 2 we get that $Z_1 = X$ since every $P + e$ contains an $s, r$-path not containing 432. Thus by Lemma 2, $p_{432} = \text{Prob}(X) = p^5p_1(1 - p)^3(1 - p_2)$. A similar argument with $P'$ shows that $d_{531} = \text{Prob}(X') = p^5p_2(1 - p)^3(1 - p_1)$.

Thus $\hat{d} \leq \min\{d_{432}, d_{531}\} = p^5(1 - p)^3(\min\{p_1, p_2\} - p_1p_2) = d'$. To see that equality holds, consider $d_I$ for other sets $I$ such that $A^* - I$ is finite. Observe first that if $I$ contains no instruction contained in $P$ or $P'$, then every instruction contained in $C$ is in $A^* - I$ and is essential for $A^* - I$, so that $A^* - I$ is not finite. Moreover, if $I$ contains one of 432 or 531, then it follows by monotonicity that $d_I \geq d'$ as desired.

Suppose now that $I$ contains an instruction $uvw$ contained in $P$ other than 432. We again have $P_1 = P$, but in every case there is also a different $s, r$-path $P_2$ containing $uvw$. Thus $d_I \geq \text{Prob}(Z_1 \cap Z_2) > \text{Prob}(X) = d_{432} \geq \hat{d}$. A similar argument shows that if $I$ has an instruction contained in $P'$ other than 531, then $d_I > \text{Prob}(X') \geq \hat{d}$.

It follows that $\hat{d} = d' = p^5(1 - p)^3(\min\{p_1, p_2\} - p_1p_2)$. Specifically, if $p = p_1 = p_2$, then $\hat{d} = p^6(1 - p)^4$.

Combining this example with Proposition 3 and the observation that neither of $s_1, s_2$ is in an essential circuit we obtain the following proposition which we will use in Section 7.

**Proposition 4.** Let $H_1, H_2$ be series-parallel graphs and $G$ be the graph obtained from $B_0 - \{s_1, s_2\}$ by identifying $s$ in $H_1, H_2$ with $s$, and identifying $r$ in $H_1, H_2$ with 1 and 2 respectively as shown in Figure 2. If $p \in (0, 1)$ is fixed and $p_i = \rho(H_i, p)$, then $\hat{d}(G, p) = p^5(1 - p)^3(\min\{p_1, p_2\} - p_1p_2)$.

**Proof.** $\hat{d}(G, p) = \rho(G, p) - \hat{\rho}(G, p) = \rho(B_0, p') - \hat{\rho}(B_0, p') = \hat{d}(B_0, p') = p^5(1 - p)^3(\min\{p_1, p_2\} - p_1p_2)$. \qed

6. Crossings of protocol reliability functions

It is natural ask if for given graphs $G, H$ it must be the case that $\hat{\rho}(G, p) < \hat{\rho}(H, p)$ for all $p \in (0, 1)$ or $\hat{\rho}(H, p) < \hat{\rho}(G, p)$ for all $p \in (0, 1)$. We will adapt an idea of Kelmans to show that this need not be the case in a very strong sense. Following his approach we let $\Delta_\rho(G, H) = \rho(G, p) - \rho(H, p)$, $\Delta_\hat{\rho}(G, H) = \hat{\rho}(G, p) - \hat{\rho}(H, p)$ and we say that the profile of a function is $(m_1, m_2, \ldots, m_k)$ if it has exactly $t$ zeroes $x_1, \ldots, x_t$ in $(0, 1)$ with $0 < x_1 < x_2 < \cdots < x_t < 1$ and $x_i$ has multiplicity $m_i$. In this language our original question is whether the profile of $\Delta_\hat{\rho}(G, H)$ must be empty. The following lemma now gives a simple negative answer for our question.

**Lemma 3.** If $G = P_k$ and $H = P_{k+1} | P_{k+1}$ for $k \geq 2$, then $\Delta_\hat{\rho}(G, H)$ has profile $(1)$ with zero $x_1 = \gamma_k$ the unique root of $f_k(p) = p^k + p^{k-1} + \cdots + p^2 + p - 1$ in $(0, 1)$.
Proof. Since $G$ and $H$ are series-parallel, it follows that
\[ \Delta_\rho(G, H) = \Delta_\rho(G, H) = \rho(P_k) - \rho(P_{k+1})|P_{k+1}| = p^{k-1} - [2p - p^2] = p^{k-1}(p - 1)f_k(p). \]
The profile of this function is the profile of $f_k$, which has a unique root $\gamma_k$ of multiplicity 1 in $(0,1)$, since $f_k(0) = -1, f_k(1) = k - 1 > 0$ and $f'_k$ is positive on $(0,1)$. 

The main idea to show that our original question has a negative answer in a much stronger sense is

**Theorem 1** (Kelmans [3], 4.1). If $H_1 = (F_1 \circ G_1) || (G_2 \circ F_2)$ and $H_2 = (F_1 \circ G_2) || (G_1 \circ F_2)$, then $\Delta_\rho(H_1, H_2) = \Delta_\rho(F_1, F_2) \cdot \Delta_\rho(G_1, G_2)$.

Observe that if $F_1, F_2, G_1, G_2$ are all series-parallel in this statement, then so are $H_1$ and $H_2$, and we also get $\Delta_\rho(H_1, H_2) = \Delta_\rho(F_1, F_2) \cdot \Delta_\rho(G_1, G_2)$. We can view this pair $(H_1, H_2)$ as a natural composition $(F_1, F_2) \cdot (G_1, G_2)$ of the pairs $(F_1, F_2)$ and $(G_1, G_2)$. Thus if we compose the pair $(P_k, P_{k+1})|P_{k+1}|$ from Lemma 2 with itself $m_k$ times we get a pair of graphs $(G_k, H_k)$ with profile $(m_k)$ for $\Delta_\rho = \Delta_\rho$, where the unique root $\gamma_k$ has multiplicity $m_k$. Since $0 = f_k(\gamma_k) < f_{k+1}(\gamma_k)$ for all $k \geq 2$ it follows moreover that $\gamma_2 > \gamma_3 > \ldots$. So if we take such pairs $(G_k, H_k)$ for $2 \leq k \leq t + 1$ and compose them with each other we get a pair $(G, H)$ with profile $(m_{t+1}, m_t, \ldots, m_3, m_2)$ and $m_k$ is the multiplicity of the root $\gamma_k$. Relabeling the subscripts now we have proved the following.

**Theorem 2.** For every $t$-tuple of positive integers $(m_1, m_2, \ldots, m_t)$ there are series-parallel graphs $H_1, H_2$ such that $\Delta_\rho(H_1, H_2) = \Delta_\rho(H_1, H_2)$ has profile $(m_1, m_2, \ldots, m_t)$.

### 7. Piecewise Polynomial Optimal Reliability Functions

As we observed in Section 3, $\hat{\rho}(G, p)$ can be achieved by different protocols for different $p$, so that $\hat{\rho}$ may be piecewise polynomial. For us a breakpoint of order $m$ in a piecewise polynomial function $f$ will be a $z \in (0,1)$ such that $f$ is differentiable $m - 1$ times at $z$, but not $m$ times, where 0 times differentiable means continuous at $z$. Equivalently there are different polynomials $p_1, p_2$ and $\varepsilon > 0$ such that $f(x) = p_1(x)$ for $x \in (z - \varepsilon, z]$ and $f(x) = p_2(x)$ for $x \in [z, z + \varepsilon)$, and $p_1(x) - p_2(x)$ has a zero of order $m$ at $x = z$. Observe that $\min\{p_1(x), p_2(x)\}$ has a breakpoint (of order $m$) at $z$ if and only if $p_1(x) - p_2(x)$ has a zero of odd order $m$ at $x = c$.

**Theorem 3.** For every $t$-tuple of positive odd integers $(m_1, m_2, \ldots, m_t)$ there is a graph $G$ so that $\hat{\rho}(G, p)$ is a piecewise polynomial with exactly $t$ breakpoints $x_1 < x_2 < \cdots < x_t$ in $(0,1)$ such that $x_i$ has order $m_i$.

Proof. Let $(H_1, H_2)$ be the series parallel graphs with profile $(m_1, m_2, \ldots, m_t)$ for $\Delta_\rho$ obtained from Theorem 2. Expanding $B_0$ at $s1, s2$ by $H_1, H_2$ as in Proposition 4 we obtain a graph $G$ with $\hat{d}(G, p) = p^{3}(1 - p)^{3}(\min\{p_1, p_2\} - p_1p_2)$ where $p_i = \rho(H_i, p)$. This function has a breakpoint of order $m$ if and only if $p_1 - p_2$ has a zero of multiplicity $m$, where $m$ is odd. \(\square\)
Remark 1. Every breakpoint is an algebraic number, so not every number in (0,1) is a breakpoint of some \( \hat{\rho}(G, p) \), but by using suitable graphs of the form \( P_{i_1} || P_{i_2} || \cdots || P_{i_k} \) for \( H_1, H_2 \) in Theorem 3 it should be possible to prove that the set of breakpoints is dense in (0,1).

The next theorem gives infinitely many small intervals that do not contain breakpoints for \( \hat{\rho}(G, p) \).

**Theorem 4.** For any rational \( \frac{a}{b} \in [0, 1] \), \( \hat{\rho}(G, p) \) has no breakpoint \( p \) with \( 0 < |p - \frac{a}{b}| < (3b)^{-|E(G)|} \).

**Proof.** Let \( m = |E(G)| \) and \( c = \frac{a}{b} \). It is sufficient to show that if \( A, A' \) are finite protocols with \( \rho_A(G, p) \neq \rho_{A'}(G, p) \), then the polynomial \( f(x) = \rho_A(G, x + c) - \rho_{A'}(G, x + c) \) has no zero \( x \) with \( |x| < (3b)^{-m} \). Observe that for every protocol \( A \) we can write \( \rho_A(G, p) = \sum_{i=0}^{m} a_i p^i (1-p)^{m-i} \) where \( a_i \) is the number of sets on \( i \) edges that contain an \( A \)-walk. Thus \( 0 \leq a_i \leq \binom{m}{i} \) and it follows that for some \( b_i \) with \( |b_i| \leq \binom{m}{i} \)

\[
f(x) = \sum_{i=0}^{m} b_i (x+c)^i (1-c-x)^{m-i} = \sum_{i=0}^{m} \sum_{j=0}^{m-i} b_i \binom{i}{j} x^j c^{i-j} (m-i) \binom{m-i}{\ell} (-x)^\ell (1-c)^{m-i-\ell}
\]

\[
= \sum_{r=0}^{m} \sum_{j=0}^{m-r+j} \sum_{i=j}^{m-i} x^r b_i \binom{i}{j} c^{i-j} \binom{m-i}{r-j} (-1)^{r-j} (1-c)^{m-r-(i-j)}
\]

\[
= \sum_{r=0}^{m} x^r \sum_{j=0}^{m-r} \sum_{s=0}^{m-r-j} (-1)^{r-j} b_{s+j} \binom{s+j}{j} \binom{m-s-j}{r-j} c^s (1-c)^{m-r-s} = \sum_{r=0}^{m} c_r x^r,
\]

where we used the substitutions \( r = \ell + j \) and \( s = i - j \). Observe that \( 1-c = \frac{b-a}{b} \) so that \( c_r \) is rational with denominator \( b^{m-r} \leq b^m \) and we have that \( |c_r| \geq b^{-m} \) unless \( c_r = 0 \). Thus

\[
|c_r| \leq \sum_{j=0}^{r} \sum_{s=0}^{m-r} |b_{s+j}| \binom{s+j}{j} \binom{m-s-j}{r-j} c^s (1-c)^{m-r-s}
\]

\[
\leq \sum_{j=0}^{r} \sum_{s=0}^{m-r} \binom{m}{s+j} \binom{s+j}{j} \binom{m-s-j}{r-j} c^s (1-c)^{m-r-s}
\]

\[
= \sum_{j=0}^{r} \sum_{s=0}^{m-r} \binom{m}{r} \binom{r}{j} \binom{m-r}{s} c^s (1-c)^{m-r-s}
\]

\[
= \sum_{j=0}^{r} \binom{m}{r} \binom{r}{j} (c+1-c)^{m-r} = \binom{m}{r} 2^r < \sum_{r=0}^{m} \binom{m}{r} 2^r 1^{m-r} = 3^m.
\]

If the degree of \( f \) is \( \alpha \), then \( g(x) = x^\alpha f(\frac{1}{x}) \) is a polynomial with leading coefficient \( c_\beta \neq 0 \), so by Cauchy's bound \( \prod_{r \leq m/2} \frac{1}{|r|^{\alpha}} \) every zero \( z \) of \( g \) satisfies \( |z| \leq 1 + \max\{|c_r/c_\beta| : 0 \leq r \leq m\} \leq 3^m / (1/b^m) = (3b)^m \) and thus the nonzero roots of \( f \) are bounded below by \( (3b)^{-m} \). \( \square \)
8. Reliable protocols for probabilities near zero

Determining \( \hat{\rho}(G,p) \) for all values of \( p \) appears to be a difficult problem, however there is something we can say for \( p \) close to zero. There must be a protocol \( A_0 \) and an \( \varepsilon > 0 \) such that \( \hat{\rho}(G,p) = \rho_{A_0}(G,p) \) for all \( p \in [0, \varepsilon) \), and we call this the optimal protocol near zero. Near zero a good protocol \( A \) will have many short \( A \)-paths. Consider \( A^{(m)} = \{uvw : uvw \text{ is contained in some } s, r \text{-path of length } \leq m \} \) and let \( d(u,v) \) denote the distance between \( u \) and \( v \) in \( G \).

**Theorem 5.** If \( k = d(s,r) \) and \( d_i \) is the number of \( s, r \text{-paths of length } i \), then \( A_0 \supseteq A^{(k+1)} \) and \( \hat{\rho}(G,p) = \rho_{A_0}(G,p) = d_k p^k + d_{k+1} p^{k+1} + O(p^{k+2}) \) for all \( p < 3^{-m} \), where \( m = |E(G)| \).

**Proof.** Observe that if we let \( p = 1 - q \), for every protocol \( A \) we can let \( \rho_A(G,p) = \sum_{i=0}^{m} a_i p^i q^{m-i} \) where \( a_i \) is the number of sets on \( i \) edges that contains an \( A \)-walk. Observe that \( a_i = 0 \) for all \( i < k \) and \( a_k \leq d_k \), since every \( A \)-walk contains an \( s, r \)-path. The optimal protocol near zero must have \( a_k \) as large as possible (as \( p^k q^{m-k} \) is the dominant term), and subject to that it must have \( a_{k+1} \) as large as possible (and so on.) Since every \( A \)-walk on a set at most \( k + 1 \) edges must contain an \( s, r \)-path of length at most \( k + 1 \) we conclude that \( A_0 \supseteq A^{(k+1)} \) if the latter is a finite protocol. If this the case, then we see that for \( A_0 \) we have \( a_k = d_k \) (as every \( s, r \)-path of length \( k \) is now an \( A_0 \)-walk) and \( a_{k+1} = d_{k+1} + (m - k)d_k \) since every set of \( k + 1 \) edges containing an \( s, r \)-walk must either be an \( s, r \)-path of length \( k + 1 \) or an \( s, r \)-path of length \( k \) and one additional edge. Thus

\[
\rho_{A_0}(G,p) = d_k p^k (1 - p)^{m-k} + (d_{k+1} + (m - k)d_k) p^{k+1} (1 - p)^{m-k-1} + O(p^{k+2}) = d_k p^k + d_{k+1} p^{k+1} + O(p^{k+2}).
\]

The bound of \( 3^{-m} \) follows from Theorem 4 with \( \frac{q}{p} = \frac{\varepsilon}{1} \). It remains to see that \( A^{(k+1)} \) is finite. This will follow if we can show that for all \( uvw \in A^{(k+1)} \) we have \( d(s,u) < d(s,v) \) since the distance from the vertices in an essential circuit to \( s \) would have to increase for every two steps along the circuit, but eventually we will repeat a vertex as we continue along the circuit. So suppose that \( d(s,u) \geq d(s,v) \) and let \( Q \) be a path of length at most \( k + 1 \) that contains the instruction \( uvw \). The length of the \( s,w \) segment of \( Q \) is at least \( d(s,u) + 2 \) and so if we replace this segment by a shortest \( s,w \)-path, then we get an \( s, r \)-walk of length at most \( (k + 1) - (d(s,u) + 2) + d(s,w) \leq k - 1 \), a contradiction. \( \square \)

9. Reliable protocols for probabilities near one

As we observed previously, for every protocol \( A \) we can let \( \rho_A(G,p) = \sum_{i=0}^{m} a_i p^i q^{m-i} \) where \( a_i \) is the number of sets on \( i \) edges that contains an \( A \)-walk. The optimal protocol near one must have \( a_m \) as large as possible (as \( p^m q^0 \) is the dominant term), and subject to that it
must have $a_{m-1}$ as large as possible (and so on.) If $c_k$ is the number of edge-sets of size $k$ that is contained in some edge-cut that disconnects $s$ from $r$, then clearly $a_i \leq \binom{m}{i} - c_{m-i}$. It is the main result of [6] that if the size of a smallest edge-cut separating $s$ and $r$ is $e$, then there is a finite protocol $A'$ such that there is an $A'$-walk in $G$ unless at least $e + 1$ edges fail or the $e$ edges of a minimum cut separating $s$ and $r$ fail. So if we let $A_1$ be the optimal finite protocol near one then for $A_1$ we get $a_i = \binom{m}{i} - c_e$ for all $i > m - e$, where $c_e$ simply counts the number of edge-cuts of minimum size $e$ that separate $s$ from $r$.

It now follows that

$$
\rho_{A_1}(G, p) = \sum_{i=0}^{m} a_i p^i q^{m-i} = \sum_{i=m-e}^{m} \binom{m}{i} p^i q^{m-i} - c_e (1 - q)^{m-e} q^e + O(q^{e+1})
$$

$$
= \sum_{i=0}^{m} \binom{m}{i} p^i q^{m-i} - c_e q^e + O(q^{e+1}) = (p + q)^m - c_e q^e + O(q^{e+1}) = 1 - c_e q^e + O(q^{e+1}).
$$

This proves the following counterpart to Theorem 5 for the optimal protocol for probabilities near one.

**Theorem 6.** $\hat{\rho}(G, p) = \rho_{A_1}(G, p) = 1 - c_e q^e + O(q^{e+1})$ for $q < 3^{-m}$.

To improve on this result in general would require a better understanding of the notion of robustness studied in [6]. A protocol $A$ is called $k$-robust if it is finite, and for every set $E$ of at most $k$-edges that does not disconnect $s$ from $r$, there is an $A$-walk in $G - E$. In a $k$-robust protocol we have $a_{m-k} = \binom{m}{i} - c_i$ for all $i \leq k$, and the optimum protocol $A_1$ near one must have maximum robustness. Thus studying the properties of $A_1$ can be viewed as a refinement of the approach in [6].

10. OPEN PROBLEMS

Computing $\hat{\rho}(G, p)$ exactly is likely to be a very hard problem in general, since Provan and Ball [9] showed that even computing $\rho(G, p)$ is $\#P$-hard.

The most interesting open question is clearly to characterize the graphs for which $\hat{\rho}(G, p)$ is a polynomial. In [8] it is shown that the 10 minor-minimal graphs $G$ for which $\hat{\rho}(G, p) < \rho(G, p)$ all have the property that $\hat{\rho}(G, p)$ is polynomial, so such a characterization could be quite difficult to obtain. One point of inquiry could be to find all graphs for which $\hat{\rho}(G, p) = \rho_{A^* -I}(G, p)$ where $I$ is a single instruction.

Can we give a polynomial time procedure for determining $\hat{\rho}(G, p)$ exactly for a fixed $p$, or near 0 or near 1?

**ACKNOWLEDGEMENTS**

The first author thanks Johan Rosenkilde for a helpful discussion that led to Theorem 4.
REFERENCES

[1] A. L. Cauchy, *Œuvres complètes. Series 2. Volume 9*, Cambridge Library Collection, Cambridge University Press, Cambridge, 2009. Reprint of the 1891 original.

[2] C. J. Colbourn, *The combinatorics of network reliability*, International Series of Monographs on Computer Science, The Clarendon Press, Oxford University Press, New York, 1987.

[3] F. E. Fich, A. Kündgen, M. J. Pelsmajer, and R. Ramamurthi, *Graph minors and reliable single message transmission*, SIAM J. Discrete Math., 19 (2005), pp. 815–847.

[4] C. Graves and D. Milan, *Reliability polynomials having arbitrarily many inflection points*, Networks, 64 (2014), pp. 1–5.

[5] A. K. Kelmans, *Crossing properties of graph reliability functions*, J. Graph Theory, 35 (2000), pp. 206–221.

[6] A. Kündgen, M. J. Pelsmajer, and R. Ramamurthi, *k-robust single-message transmission*, SIAM J. Discrete Math., 24 (2010), pp. 301–321.

[7] E. F. Moore and C. E. Shannon, *Reliable circuits using less reliable relays. I, II*, J. Franklin Inst., 262 (1956), pp. 191–208, 281–297.

[8] J. S. P. Patno, *Communication Networks*, M.Sc. thesis, California State University San Marcos, 2011.

[9] J. S. Provan and M. O. Ball, *The complexity of counting cuts and of computing the probability that a graph is connected*, SIAM J. Comput., 12 (1983), pp. 777–788.

[10] D. B. West, *Introduction to graph theory*, Prentice Hall, Inc., Upper Saddle River, NJ, second ed., 2001.

[11] A. Younes and M. R. Girgis, *A tool for computing computer network reliability*, Int. J. Comput. Math., 82 (2005), pp. 1455–1465.