FAULT TOLERANCE OF CAYLEY GRAPHS

SHUHONG GAO AND BETH NOVICK

ABSTRACT. It is a difficult problem in general to decide whether a Cayley graph $\mathrm{Cay}(G;S)$ is connected where G is an arbitrary finite group and S a subset of G. For example, testing primitivity of an element in a finite field is a special case of this problem but notoriously hard. In this paper, it is shown that if a Cayley graph $\mathrm{Cay}(G;S)$ is *known* to be connected then its fault tolerance can be determined in polynomial time in $|S|\log(|G|)$. This is accomplished by establishing a new structural result for Cayley graphs. This result also yields a simple proof of optimal fault tolerance for an infinite class of Cayley graphs, namely exchange graphs. We also use the proof technique for our structural result to give a new proof of a known result on quasiminimal graphs.

1. INTRODUCTION

Let G be any group and S a subset of G not containing the identity 1. We define a *Cayley digraph*, denoted $\mathrm{Cay}(G;S)$, to have elements of G as vertices and, for any two vertices $x, y \in G$, a directed edge $[x,y]$ if $x \cdot s = y$ for some $s \in S$. When $S = S^{-1}$, where $S^{-1} = \{s^{-1} \mid s \in S\}$, the directed graph $\mathrm{Cay}(G;S)$ can be viewed as an undirected graph, called a Cayley graph, as there is an edge in each direction between two vertices whenever there is one between them. The underlying undirected graph of a Cayley digraph can be represented as a Cayley graph. Cayley graphs were first introduced by Cayley [5] as diagrams representing a group in terms of its generators. Cayley graphs, both in their directed and undirected form have been widely studied. For algebraic properties of Cayley graphs, see for example the papers [3, 17, 18].

A communication interconnection network can be modelled as a (directed or undirected) graph whose vertices correspond to processors or communication nodes, and whose edges correspond to communication channels, see [1, 21]. For designing these networks it is desirable to use graphs that are highly symmetric. A Cayley graph is vertex transitive, so symmetric in the sense that it looks the same when viewed from any vertex. Cayley graphs are therefore attractive candidates for the design of communications networks. Some other important features of a communications network are small degree, small diameter, and high connectivity (and hence high 'fault tolerance'). Cayley graphs have many of these features and tend to yield excellent routing algorithms as well; see for example [9, 10] for Cayley graphs on abelian groups. In this paper we focus on *fault tolerance*, namely the largest number k such that the failure of any k nodes does not destroy the connectivity of the entire network.

A digraph is *strongly connected* if for every ordered pair (x,y) of vertices, there is at least one directed path, or dipath, from x to y. A Cayley digraph $\mathrm{Cay}(G;S)$, for finite G, is strongly connected iff S generates the group G. We consider primarily strongly connected Cayley graphs. The *connectivity* of a digraph is the smallest number k so that there exist k vertices in the graph

Date: March 10, 2006.

The first author was supported in part by National Science Foundation (NSF) under Grant DMS0302549, and the DoD Multidisciplinary University Research Initiative (MURI) program administered by the Office of Naval Research (ONR) under Grant N00014-00-1-0565.

whose removal leaves a digraph that is either no longer strongly connected or consisting of a single vertex. Denote the connectivity of a graph $\mathcal{X}$ by $\kappa(\mathcal{X})$. The fault tolerance of $\mathcal{X}$ is then $\kappa(\mathcal{X})-1$. Hence a network with fault tolerance k remains strongly connected with any k or fewer nodes broken. Our Cayley graph $\mathcal{X} = \mathrm{Cay}(G;S)$ is regular in the sense that each vertex has out-degree and in-degree both equal to $|S|$. Clearly $\kappa(\mathcal{X}) \leq |S|$. When equality holds, $\mathrm{Cay}(G;S)$ has highest possible connectivity, which means optimal fault tolerance.

For any digraph $\mathcal{X}$ and any vertex cut $C \subseteq V(\mathcal{X})$, the strongly connected components of $\mathcal{X} \setminus C$ are called the *fragments* of $\mathcal{X}$ induced by C. A fragment is called an *atom* if it is induced by a vertex cut of minimum cardinality and it has minimum cardinality among all such fragments. For any subset A of $V(\mathcal{X})$, we denote

$$\begin{aligned} N^+(A) &= \{v \in V(\mathcal{X}) \setminus A : [u,v] \in E(\mathcal{X}) \text{ for some } u \in A\}, \text{ and} \\ N^-(A) &= \{v \in V(\mathcal{X}) \setminus A : [v,u] \in E(\mathcal{X}) \text{ for some } u \in A\}, \end{aligned}$$

called the positive or negative neighborhood of A, respectively. An atom A is called *positive* or *negative* depending on whether $N^+(A)$ or $N^-(A)$ is a vertex cut (of minimum cardinality). Every Cayley digraph contains an atom, although it may not contain a positive one. By replacing S with S^{-1} if necessary, we may assume that our Cayley digraph $\mathrm{Cay}(G;S)$ has a positive atom.

In 1970 Watkins [22] established the fundamental result that for any connected graph (undirected), distinct atoms are disjoint. In the same paper he showed that, for any vertex transitive graph, every atom is vertex-transitive and the atoms are isomorphic subgraphs that form a partition of G. Watkins' results are for the undirected case, and Hamidoune [13] showed in 1977 that for a vertex transitive digraph the analogous results hold. In a later paper Hamidoune [14] showed further that for any Cayley digraph $\mathrm{Cay}(G;S)$ the atom A containing the identity 1 is a subgroup of G and is generated by $A \cap S$. Our main result, established in Section 2, extends these structural properties, namely we show that A is actually contained in the set $S \cdot S^{-1} = \{a \cdot b^{-1} : a, b \in S\}$.

In Section 3, we show how our structural result gives an efficient algorithm for computing the fault tolerance of Cayley graphs $\mathrm{Cay}(G;S)$. We assume that the group G is given by an *oracle* (or a *black box*). The oracle can perform various group operations, namely, product of two elements, the inverse of an element, and distinctness of two elements. The running time of our algorithm is measured by the number of calls to the oracle. We show that our algorithm runs in time polynomial in $|S|$, the degree of the graph, assuming $\mathrm{Cay}(G;S)$ is strongly connected. We show that one advantage of this model is that for any specific group G, if each element of G is represented using $\mathcal{O}(\log|G|)$ bits and each group operation of G can be computed in time polynomial in $\log|G|$, then our algorithm can be implemented so that its running time is polynomial in $|S|\log(|G|)$.

We should remark that the problem of determining whether two given words represent the same group element is known as the "word problem for groups" and, while easy in practice for many groups, is undecidable in general: it has been proven that there is no algorithm that will solve the group word problem for all groups, [4, 20]. In our situation, the oracle described above is assumed to have the superpower of solving the word problem, hence our work is not meant to shed any light on the word problem.

We should also remark that deciding whether a given Cayley graph is strongly connected is in general hard. For example, if G is the multiplicative group of a finite field, then for any element $a \in G$, the Cayley graph $\mathrm{Cay}(G;\{a,a^{-1}\})$ is (strongly) connected if and only if a is a primitive element of the field (i.e., each nonzero element of the field is a power of a). Testing primitivity is, however, a notoriously hard problem. Our algorithm does not solve this problem. Instead it finds the fault tolerance (or connectivity) of each strongly connected component of $\mathrm{Cay}(G;S)$. Hence

if a Cayley graph $\mathrm{Cay}(G;S)$ is known to be strongly connected, then our algorithm finds its fault tolerance.

As further application of our structural result, we show in Section 4 that exchange graphs have optimal fault tolerance. Also in Section 4 we obtain a result regarding quasiminimal graphs, namely that all but a particular family of quasiminimal graphs have optimal fault tolerance. This result was established in its undirected form by Alspach [2] and in its directed form by Hamidoune, Lladó and Serra [15]. We give a proof of a somewhat different flavor using a proof technique similar to that used to establish our structural result in Section 3. We note that in a subsequent paper J. Morris further studied and characterized this family of quasiminimal Cayley graphs, see [19]. So while the result is not new, the authors of the present paper find the proof to be an interesting application of the proof techniques involved.

2. Properties of atoms

For any group G and any subset H of G, we denote by $\langle H \rangle$ the subgroup of G generated by the elements in H. When H is empty, $\langle H \rangle$ denotes the trivial group $\{1\}$ consisting of the identity only. The following two results summarize what is known about the properties of the atoms of Cayley graphs. For completeness, and because they are scattered in different papers, we include their proofs here.

Theorem 1 (Hamidoune [13] and Watkins [22])**.** *Let $\mathcal{X}$ be any strongly connected digraph with a positive atom. Then its positive atoms form a disjoint partition of all the vertices.*

Proof. Assume to the contrary that there are distinct positive atoms A and B with $A \cap B \neq \emptyset$. Since $A \cap B$ is smaller than A (or B), it is not an atom. There are two cases:

(a) Each element of G is contained in $A \cap B$ or $N^+(A \cap B)$;
(b) $N^+(A \cap B)$ is a vertex cut that is not minimum.

But the case (a) would imply that $N^+(A) \cup A$ is the entire graph, contradicting the fact that $N^+(A)$ is a vertex cut. So (b) holds and $|N^+(A \cap B)| > \kappa$, where $\kappa = \kappa(G;S)$. Let

$$A_1 = N^+(B) \cap A, \quad B_1 = N^+(A) \cap B, \quad \text{and} \quad D = N^+(A) \cap N^+(B).$$

Since $N^+(A \cap B) \subseteq A_1 \cup B_1 \cup D$, we have $|A_1| + |B_1| + |D| > \kappa$. Let

$$A_2 = N^+(A) \setminus (D \cup B) \quad \text{and} \quad B_2 = N^+(B) \setminus (D \cup A).$$

Since $N^+(B) = A_1 \cup D \cup B_2$ we have

$$|N^+(B)| = \kappa = |A_1| + |D| + |B_2| < |A_1| + |B_1| + |D|,$$

which implies that $|B_2| < |B_1|$. It follows that

$$|A_2| + |D| + |B_2| < |A_2| + |D| + |B_1| = |N^+(A)| = \kappa,$$

and therefore $A_2 \cup D \cup B_2$ cannot be a vertex cut. In other words, since $A_2 \cup D \cup B_2 = N^+(A \cup B)$, the entire vertex set is $(A_2 \cup D \cup B_2) \cup (A \cup B)$. Let $\tilde{A}$ be the set of all vertices in the complement of $A \cup N^+(A)$. Then $\tilde{A} \subsetneq (B \setminus B_1) \cup B_2$ and so $|\tilde{A}| < |B| - |B_1| + |B_2| < |B|$, implying that $\tilde{A}$ contains a fragment of $N^+(A)$ that is smaller than an atom, a contradiction. □

Theorem 2 (Hamidoune [14])**.** *Let G be any finite group and S a subset of G not containing the identity 1. Assume that the Cayley graph $Cay(G;S)$ contains positive atoms. Let A be the positive atom of $Cay(G;S)$ containing 1. Then A is a subgroup of G and $A = \langle S \cap A \rangle$. Furthermore, every positive atom is of the form aA, $a \in G$, i.e. a left coset of A.*

Proof. First note that for any $a \in G$, aA is also an atom, as multiplication on the left by a on G induces a graph automorphism. To prove that A is a subgroup it suffices to show that it is closed under multiplication, since A is finite. For any $a \in A$, since $1 \in A$, we have $a \in aA \cap A$. Hence aA and A must be identical atoms, namely $aA = A$ for every $a \in A$, establishing the closure of A under multiplication.

It remains to show that A is generated by $S \cap A$. For any two vertices $x, y \in A$, suppose there is an edge from x to y, say $x \cdot s = y$ for some $s \in S$. Since A is a group, it follows that $s \in A$. Hence all the edges in the subgraph induced by A are generated by elements in $S \cap A$. We claim that this subgraph is strongly connected. Indeed, if we assume to the contrary that $x, y \in A$ but that A contains no dipath from x to y, then the set of all vertices in A reachable from x comprises a positive fragment smaller than $|A|$, contradicting the fact that A is atomic. Hence for each element $a \in A$, there is a dipath from 1 to a, which means that a is a product of elements in $S \cap A$. This proves that A is generated by $S \cap A$. □

Before presenting our improvement on Theorem 2, we give a simple lemma.

Lemma 3. *Let B be a subset of a finite group A with $|B| > \frac{1}{2}|A|$. Then*

$$A = B \cdot B^{-1} = \{a \cdot b^{-1} : a, b \in B\}.$$

Proof. Since A is a group, we have $B \cdot B^{-1} \subseteq A$. To establish the reverse inclusion, consider any $a \in A$. Since aB and B are subsets of A having cardinality greater than $\frac{1}{2}|A|$, we have $|aB| + |B| > |A|$ and thus $aB \cap B \neq \emptyset$, implying the existence of elements $b_1, b_2 \in B$ with $b_1 = a \cdot b_2$, i.e. $a = b_1 \cdot b_2^{-1}$. It follows that $a \in B \cdot B^{-1}$ for each $a \in A$, so $A = B \cdot B^{-1}$. □

Theorem 4. *Let $\mathcal{X} = Cay(G; S)$ be any finite Cayley graph with a positive atom A containing the identity 1. Then A is contained in $S \cdot S^{-1}$.*

Proof. If $\kappa(\mathcal{X}) = |S|$, then $A = \{1\}$ and the theorem is trivial in this case. Hence we assume that $\kappa(\mathcal{X}) < |S|$. By Theorem 1, A is a subgroup of G, hence the vertex cut $N^+(A)$ is a disjoint union of distinct right cosets of A, say $Ab_1, Ab_2, \ldots, Ab_\ell$, where $b_1, b_2, \ldots, b_\ell \in S \setminus A$. So we have

$$\kappa(\mathcal{X}) = |N^+(A)| = \ell|A| < |S|.$$

Let $d_0 = |S \cap A|$ and let $d_i = |S \cap Ab_i|$ for $i = 1, \cdots, \ell$. Since $S \subseteq A \cup N^+(A)$, we have

$$d_0 + d_1 + \cdots + d_\ell = |S|.$$

We claim that there is an $0 \leq i \leq \ell$ with $d_i > \frac{1}{2}|A|$. Indeed, if $d_i \leq \frac{1}{2}|A|$ for all $1 \leq i \leq \ell$, then

$$|S| \leq d_0 + \frac{\ell}{2}|A|,$$

which, together with the fact that $\ell|A| < |S|$, implies that

$$d_0 \geq |S| - \frac{\ell}{2}|A| > \ell|A| - \frac{\ell}{2}|A| = \frac{\ell}{2}|A| \geq \frac{1}{2}|A|.$$

Therefore, $|Ab_i \cap S| > \frac{1}{2}|A|$ for some $0 \leq i \leq \ell$ where $b_0 = 1$. Let B be the subset of A such that $Ab_i \cap S = Bb_i$. Then $|B| = |Ab_i \cap S| > \frac{1}{2}|A|$. By the above lemma, we have

$$A = B \cdot B^{-1} = (Bb_i) \cdot (Bb_i)^{-1} = (Ab_i \cap S) \cdot (Ab_i \cap S)^{-1} \subseteq S \cdot S^{-1}.$$

This completes the proof. □

3. Algorithm for computing fault tolerance

Let G be any finite group, given by an oracle as described earlier in the introduction, and S any subset of G. The Cayley graph $\mathcal{X} = \mathrm{Cay}(G; S)$ may not be strongly connected, but its strongly connected components are isomorphic. Let G_0 be the subgroup generated by S. Then the Cayley graph $\mathrm{Cay}(G_0; S)$ is the connected component of $\mathcal{X}$ that contains the identity 1. We denote this component by $\mathcal{X}_0$, i.e., $\mathcal{X}_0 = \mathrm{Cay}(G_0; S)$. We show how to compute the fault tolerance of $\mathcal{X}_0$ by using the oracle for group operations. The basic idea is to construct a smaller graph whose size is bounded by a polynomial in $|S|$ and in which certain maximum flow is equal to the connectivity of the original graph $\mathcal{X}_0$. We then apply any one of the efficient algorithms in the literature, for which we give references later, to this new graph in order to compute its connectivity. The fault tolerance is simply the connectivity minus 1.

First we need to construct the desired new digraph, call it $\overline{\mathcal{X}}_0$. Define

$$\begin{aligned} A_1 &= S \cdot S^{-1} = \{s_1 s_2^{-1} \,:\, s_1, s_2 \in S\}, \\ A_2 &= (A_1 \cdot S) \setminus A_1. \end{aligned}$$

Then

$$1 \in A_1 \quad \text{and} \quad A_1 \cup A_2 = (S \cdot S^{-1}) \cdot S.$$

The new graph $\overline{\mathcal{X}}_0$ will consist of the induced subgraph of $\mathcal{X}_0$ on the vertex subset $A_1 \cup A_2$. If $G_0 \neq A_1 \cup A_2$, we add one additional vertex, v_∞, and an additional edge $[v, v_\infty]$ for each $v \in A_2$.

The new digraph $\overline{\mathcal{X}}_0$ may be constructed by calling the oracle for G. As mentioned in the introduction, we assume that the oracle can perform various group operations, namely product of two elements, the inverse of an element, and distinctness of two elements. Let $k = |S|$. We can construct S^{-1} with k calls to the oracle. All elements of the form $a \cdot b$, $a \in S$ and $b \in S^{-1}$ require k^2 calls. Duplicates may be eliminated using at most $k^2(k^2-1)/2$ calls, since checking whether any given element lies in a set of i elements needs i calls. This gives us the vertex set A_1, which has at most k^2 elements. Finding all edges in the subdigraph induced by A_1 requires no more than $k^2(k^2-1) \cdot k$ calls. Hence A_1 can be constructed, duplicates can be removed, and edges of A_1 can be constructed by $\mathcal{O}(k^5)$ calls to the oracle. We need $\mathcal{O}(k^3)$ calls to get all the distinct elements in $A_1 \cdot S$ that are not already in A_1, this gives A_2 which has at most k^3 elements. No more than $\mathcal{O}(k^6 \cdot k)$ calls are needed to get all the edges $[a, b]$, where $a \in A_1$ and $b \in A_2$ or $a, b \in A_2$. Finally, to check whether $G_0 = A_1 \cup A_2$, we compute the set $B = (A_1 \cup A_2) \cdot S$ and compare each of its elements to each element of $A_1 \cup A_2$, which needs at most $k(k^2 + k^3)^2$ calls. If B contains no elements that are different from those in $A_1 \cup A_2$, then $A_1 \cup A_2$ is the vertex set of the connected component of $\mathrm{Cay}(G; S)$ that contains the identity, namely $G_0 = A_1 \cup A_2$. Otherwise, $G_0 \neq A_1 \cup A_2$. Hence the new graph $\overline{\mathcal{X}}_0$ can be constructed using at most $\mathcal{O}(k^7)$ calls to the oracle.

Lemma 5 below shows that finding $\kappa(\mathcal{X}_0)$ is no harder than finding $\kappa(\overline{\mathcal{X}}_0)$. If s and t are vertices in a digraph then an s-t cut is a set of vertices containing neither s nor t whose removal leaves a digraph that contains no s-t dipath. We use the directed version of Menger's theorem for vertices that states that the minimum cardinality of an s-t cut is equal to the maximum number of internally disjoint s-t dipaths, see [6].

Lemma 5. *Suppose $G_0 \neq A_1 \cup A_2$. Then $\kappa(\mathcal{X}_0)$ is equal to the cardinality of a minimum 1-v_∞ vertex cut in $\overline{\mathcal{X}}_0$.*

Proof. Let A be the positive atom of $\mathcal{X}_0$ containing the identity 1. By Theorem 4, $A \subseteq S \cdot S^{-1}$ and hence

$$N^+(A) \subseteq \left(S \cdot S^{-1}\right) \cdot S = A_1 \cup A_2.$$

In both digraphs, namely in both $\mathcal{X}_0$ and $\overline{\mathcal{X}}_0$, the vertex set $N^+(A)$ separates A from all vertices lying outside $A \cup N^+(A)$. Hence $N^+(A)$ is an 1-v_∞ cut and so the minimum cardinality of 1-v_∞ vertex cuts in $\overline{\mathcal{X}}_0$ is at most $|N^+(A)| = \kappa$.

On the other hand, $G_0 \neq A_1 \cup A_2$ by our assumption, so there is at least one vertex say x of $\mathcal{X}_0$ that is not in $A_1 \cup A_2$. By the directed version of Menger's theorem for vertex cuts, there are κ internally vertex disjoint dipaths $P_1, P_2, \cdots, P_\kappa$ from 1 to x in the larger digraph $\mathcal{X}_0$. By the construction of A_2, every path from an element in A_1 to x must pass through A_2. For $1 \leq i \leq \kappa$, let v_i be the first vertex in P_i that is in A_2 but the next vertex in P_i is outside of $A_1 \cup A_2$. Let $P(1, v_i)$ be the sub-dipath of P_i that begins at 1 and terminates at v_i. Each $P(1, v_i)$ is entirely contained in the sub-digraph induced by $A_1 \cup A_2$ and hence is a dipath in the smaller digraph, $\overline{\mathcal{X}}_0$, as well. Appending v_∞ to each $P(1, v_i)$ we obtain κ internally vertex disjoint 1-v_∞ dipaths in $\overline{\mathcal{X}}_0$, hence the minimum cardinality of 1-v_∞ vertex cuts in $\overline{\mathcal{X}}_0$ is at least κ. Therefore κ is equal to the minimum cardinality of 1-v_∞ vertex cuts in $\overline{\mathcal{X}}_0$. □

It is well known that the cardinality of a minimum s-t vertex cut for any two vertices s, t can be found in time polynomial in the number of vertices, see [6]. Indeed, Feder and Motwani [7] have an $\mathcal{O}(\sqrt{n} \cdot m \cdot \log_n(n^2/m))$ algorithm to find a minimum s-t cut, where $n = |V|$ and $m = |E|$. When $G_0 = A_1 \cup A_2$ we have $\kappa(\mathcal{X}_0) = \kappa(\overline{\mathcal{X}}_0)$ and hence we find $\kappa(\mathcal{X}_0)$ directly. As $\mathcal{X}_0$ is vertex transitive κ is equal to the minimum, over all v, of the cardinality of the smallest 1-v vertex cut, which can be found by applying Feder and Motwani's algorithm n times. We also remark that Gabow and Jordán [8] give an algorithm to find a minimum vertex cut in a digraph with in time $\mathcal{O}(\frac{m^2}{n^{1/4}} + nm)$. In any case, we have the following theorem.

Theorem 6. *Suppose a finite group G is given via an oracle which computes inverses, multiplication and distinctness of elements in G. Then for any given subset S of G, the connectivity of the strongly connected components of Cay$(G; S)$ can be computed in polynomial time, that is, the number of calls to the oracle made by the algorithm is at most $|S|^c$ for some constant c.*

If we assume, as discussed in the introduction, that each element of G is represented using $\mathcal{O}(\log |G|)$ bits and that each group operation of G can be computed in time polynomial in $\log |G|$, then each call to the oracle can be performed in time polynomial in $\log |G|$ as well. Hence it follows from Theorem 6 that the fault tolerance of $\mathrm{Cay}(G; S)$ can be computed in time at most $(|S| \log |G|)^c$ for some constant c.

4. Exchange graphs and quasiminimal graphs

As further applications of our structural result, namely Theorem 4, and of the techniques used in its proof, we show that two interesting classes of Cayley graphs have optimal fault tolerance. One such class is based on the symmetric group on n elements and our proof is very simple. The other class is the so-called quasiminimal Cayley graphs.

4.1. **Exchange Graphs.**

We define a Cayley graph on the symmetric group S_n of permutations on $\{1, 2, \cdots, n\}$ as follows. Let Γ be any graph (undirected) on the vertex set $\{1, 2, \cdots, n\}$. Each edge (i, j) of Γ corresponds to a transposition, or a 2-cycle, still denoted by (i, j), in S_n that exchanges i and j. Hence the set $E(\Gamma)$ of edges in Γ gives a subset of elements in S_n, thus defines a Cayley graph. By identifying Γ with $E(\Gamma)$, we may simply denote this Cayley graph by $(S_n; \Gamma)$. Following Godsil [12], we call such a graph an *exchange graph*. Since 2-cycles are their own inverses, the digraph $(S_n; \Gamma)$ is symmetric. Hence we equate it with the underlying undirected graph. When Γ is a tree, properties of the Cayley graph (S_n, Γ) are studied in [1]. For

a general graph Γ, Godsil [12, Chapter 3] proved that $(S_n;\Gamma)$ is connected iff Γ is connected. We show below that $(S_n;\Gamma)$ has optimal fault tolerance, namely $\kappa(S_n;\Gamma) = |E(\Gamma)|$.

Theorem 7. *If Γ is connected then $(S_n;\Gamma)$ is also connected and has connectivity $|E(\Gamma)|$.*

Proof. To show that $(S_n;\Gamma)$ is connected, it suffices to show that there is a path from 1 to every permutation in S_n. Since each permutation is a product of 2-cycles, we just need to show that each 2-cycle (i,j) is a product of 2-cycles from Γ. Note that $(i,j) = (i,v)(v,j)(i,v)$ for any three distinct vertices i, v, j. Hence a simple induction on the distance between i and j will prove that $(S_n;\Gamma)$ is connected iff Γ is connected.

Next we show that $\kappa(S_n;\Gamma) = |E(\Gamma)|$. Since the degree of each vertex in $(S_n;\Gamma)$ is $|E(\Gamma)|$, we have that $\kappa(S_n;\Gamma) \leq |E(\Gamma)|$. Suppose $\kappa(S_n;\Gamma)$ is strictly less than $|E(\Gamma)|$. Then by Theorem 4 the atom A containing 1 has size at least 2 and is a subset of

$$\Gamma \cdot \Gamma^{-1} = \{(i,j)(a,b) : (i,j),(a,b) \in E(\Gamma)\}.$$

Furthermore, A is generated by $A \cap \Gamma$ and, as $|A| \geq 2$, in particular $A \cap \Gamma \neq \emptyset$. Thus there is a 2-cycle of Γ that lies in $\Gamma \cdot \Gamma^{-1}$,and so is a product of two 2-cycles, which is absurd since the product of any two 2-cycles is either the identity, a 3-cycle, or the product of two disjoint 2-cycles. The result follows. □

4.2. **Quasiminimal Cayley Graphs.** A set S of distinct elements of a group G is called *quasiminimal* if its elements can be ordered, say

$$s_1 \prec s_2 \prec \cdots \prec s_r$$

so that the following condition is satisfied: letting $S_i = \{s_1, s_2, \cdots, s_i\}$, we have for $2 \leq i \leq r$

$$s_i^{-1} = s_{i-1} \quad \text{or} \quad \langle S_{i-1} \rangle \subsetneq \langle S_i \rangle.$$

When S is quasiminimal, $\mathrm{Cay}(G;S)$ is called a *quasiminimal Cayley graph*. We assume $1 \notin S$ and that S generates G, so $\mathrm{Cay}(G;S)$ is strongly connected.

Quasiminimal Cayley graphs have been studied by Alspach [2], Hamidoune, Lladó and Serra [16]. Alspach [2] showed that if S is a quasiminimal then, unless S belongs to a special family, $\mathrm{Cay}(G;S)$ has optimal fault tolerance. Hamidoune, Lladó and Serra [15] showed this result for the directed case. Earlier Akers and Krishnamurthy [1] obtain the same result but for Cayley graphs for which the associated group is restricted in size. The purpose of the present section is to give a somewhat different proof of the result of [15] using techniques of our Theorem 4. See [19] for a subsequent, stronger characterization of heirarchical Cayley graphs which lack optimal fault tolerance.

A generating set S for a group G is *minimal* if $\langle S \setminus \{s\} \rangle \subsetneq \langle S \rangle$ for all $s \in S$. Godsil [11] showed that if S is a minimal generating set of G then $\mathrm{Cay}(G;S)$ has optimal fault tolerance. A minimal set is always quasiminimal, but the converse may not be so. For example, let $G = \mathbb{Z}_8$ with the group operation being addition. Then it is easy to check that $S = \{4,6,3\}$ is quasiminimal in the order listed. However, it is not minimal as it strictly contains the generating set $\{4,3\}$.

A quasiminimal Cayley graph $\mathrm{Cay}(G;S)$ need not be optimally fault tolerant. For example (see Alspach [2]) let $G = \mathbb{Z}_4 \times \mathbb{Z}_2$ with addition being the group operation and let

$$S = \{(2,0),(1,0),(3,0),(1,1),(3,1)\},$$

in the order given. Note that $(2,0)$ has order 2, $(1,0)^{-1} = (3,0)$ and $(1,1)^{-1} = (3,1)$. The atom, A, containing the identity $(0,0)$ is $A = \{(2,0),(0,0)\}$, and

$$N^+(A) = \{(1,0),(3,0),(1,1),(3,1)\}.$$

So the vertex connectivity is $4 = |S|-1$. This is the smallest example in the family of quasiminimal Cayley graphs that do not have optimal fault tolerance.

We need the following property of quasiminimal sets.

Lemma 8. *Let S be a quasiminimal set of a group G, with $1 \notin S$. If all three elements a, b, and ab are contained in S then either $a^{-1} = b^2$ or $b^{-1} = a^2$.*

Proof. Let S be ordered as $\{s_1, s_2, \cdots, s_r\}$ that satisfies the quasiminimal property. Suppose $a, b, ab \in S$. Let s_i be the last of the three elements a, b, ab in this ordering. Note that any subgroup of G containing two of the three elements a, b, ab must contain the third. Hence $s_i \in \langle S_{i-1} \rangle$. So by the definition of quasiminimal we must have $s_i^{-1} = s_{i-1}$. Furthermore, s_{i-1} must itself be a member of the set $\{a, b, ab\}$ since otherwise S_{i-2} would generate S_i. Since $1 \notin S$ we have $a \neq b^{-1}$. Therefore either $ab = a^{-1}$ which implies $b^{-1} = a^2$, or $ab = b^{-1}$ implying $a^{-1} = b^2$. □

The following theorem is due to Alspach [2] in its undirected form and Hamidoune, Lladó and Serra [15] in the directed form. We give a proof with a somewhat different flavor, similar to our proof of Theorem 4.

Theorem 9 (Alspach [2], Hamidoune, Lladó and Serra [15])**.** *Let $S \subseteq G$ be quasiminimal. Then $Cay(G;S)$ has connectivity $|S|$ or $|S|-1$. In the latter case, S consists of an element a of order 2 in the center of G and pairs $\{b, b^{-1}\}$ with $b^2 = a$.*

Proof. Suppose $\kappa = \kappa(G;S) < |S|$. We just need to prove that $\kappa = |S|-1$ and S has the claimed structure. We keep the notation used in the proof of Theorem 4: A denotes the positive atom containing 1, and

$$N^+(A) = \cup_{i=1}^{\ell} Ab_i$$

where $b_i \in S \setminus A$, $1 \leq i \leq \ell$. Since $S \subseteq A \cup N^+(A)$, the condition $|S| > \kappa = |N^+(A)|$ implies that

$$|A \cap S| > \sum_{i=1}^{\ell} |Ab_i \setminus S|. \tag{1}$$

For convenience, let $A_0 = A \cap S$ and $A_1 = A \setminus A_0$. We claim that, for each $b \in S \setminus A$,

$$|Ab \setminus S| \geq |A_0| - 1. \tag{2}$$

In fact, for any $a \in A_0 = A \cap S$, if $ab \in Ab \cap S$ then we have $a, b, ab \in S$. It follows from Lemma 8 that $a = b^{-2}$ (or $ab = b^{-1}$), as $b \notin A$ and A is a group. Hence $ab \notin S$ for each $a \in A_0$ except possibly one element, namely when $a = b^{-2}$. Hence (2) holds. The above argument also shows that equality in (2) holds iff $b^{-2} \in A_0$. Furthermore, if equality holds then

$$Ab \setminus S = (A_0 \setminus \{b^{-2}\})b \quad \text{and} \quad Ab \cap S = \{b^{-1}\} \cup A_1 b. \tag{3}$$

where the latter equality follows from the fact that $A = A_0 \cup A_1$. Now the inequalities (1) and (2) imply that

$$|A_0| > \sum_{i=1}^{\ell} (|A_0| - 1) = \ell(|A_0| - 1).$$

There are only two possibilities: (a) $|A_0| = 1$ (and $\ell \geq 1$), or (b) $|A_0| > 1$ and $\ell = 1$.

First consider case (a). Since $|A \cap S| = |A_0| = 1$, the equation (1) implies that $|Ab_i \setminus S| = 0 = |A_0| - 1$ for each i, thus $|Ab \setminus S| = 0$ for each $b \in S \setminus A$. This means that $Ab \subseteq S$ for each $b \in S \setminus A$. It also implies that equality in (2) holds. Suppose $A_0 = A \cap S = \{a\}$. Then $b^{-2} = a$, so $ab = b^{-1} \in S$, for each $b \in S \setminus A$. Hence $S \setminus A$ consists of inverse pairs. For any pair $b, b^{-1} \in S \setminus A$, we have $b^{-2}, (b^{-1})^{-2} = b^2 \in A_0$ so $b^{-2} = a = b^2$. Hence $a^2 = 1$ and $A = \{1, a\}$. This proves the structure of S as claimed in the theorem.

Lastly, we prove that case (b) is impossible. Let $b = b_1$, $B_0 = Ab \cap S$ and $B_1 = Ab \setminus S$. Then

$$|A_0| + |B_0| = |S| > |Ab| = |B_0| + |B_1| \geq |B_0| + |A_0| - 1,$$

where the last inequality follows from (2). Hence

$$\kappa = |Ab| = |B_0| + |A_0| - 1 = |S| - 1.$$

One also has that $|B_1| = |A_0| - 1$, hence $b^{-2} \in A_0$. By (3),

$$B_0 = \{b^{-1}\} \cup A_1 b.$$

Note that $1 \in A_1$. We claim that $A_1 = \{1\}$. Suppose otherwise. There is an element $c \in A_1 \setminus \{1\}$. By Theorem 2, $A = A_0 \cup A_1$ is generated by A_0, so there are elements $a_1, a_2 \in A_0$ such that $c = a_1 a_2$. Hence we have four elements $a_1, a_2, b, cb \in S$. Since any three of them can generates the other, the quasiminimal property of S implies that there is at least one inverse pair among them. Since $c = a_1 a_2 \neq 1$ and b is not in the subgroup A, the only possible pair is b and cb. Hence $b^{-1} = cb$, thus $b^{-2} = c$. This contradicts with the fact that $b^{-2} \in A_0$. Therefore $A_1 = \{1\}$ and consequently $B_0 = \{b, b^{-1}\}$. Since $b^{-2} \in A_0$, $\langle b^2 \rangle \subseteq A$. If $A = \langle b^2 \rangle$ then as $Abb = Abb^{-1} = Aba = A$ for all $a \in A_0$, $N^+(A)$ contains only one part, namely A, contradicting the fact that $N^+(A)$ is a vertex cut. Hence $\langle b^2 \rangle \subsetneq A$, but then $\langle b^2 \rangle$ is a fragment of the minimum cut $(A \setminus \langle b^2 \rangle) \cup (\langle b^2 \rangle b)$ which is impossible since A is atomic. Hence the theorem is proved. □

References

[1] S. Akers and B. Krishnamurthy, "A group-theoretic model for symmetric interconnection Networks", *IEEE Transactions on Computers*, 38(1989), no. 4, 555-566.

[2] B. Alspach, "Cayley graphs with optimal fault tolerance", *IEEE Transactions on Computers*, 41(1992), no. 10, 1337-1339.

[3] L. Babai, W.M. Kantor and A. Lubotzky, "Small diameter Cayley graphs for finite simple groups", *European J. Combinatorics*, 10(1989), 507-522.

[4] W.W. Boone, F.B. Cannonito, R.L. Lyndon. *Word Problems: Decision Problem in Group Theory*, North-Holland, Netherlands, 1973.

[5] A. Cayley, "On the theory of groups", *Proc. London Math. Soc.*, 9(1878), 126-233.

[6] S. Even, *Graph Algorithms*, Computer Science Press, Inc., 1979.

[7] T. Feder and R. Motwani, "Clique partitions, graph compression and speeding-up algorithms", *Journal of Computer and System Sciences*, 51(1995), 261-272.

[8] H.N. Gabow and T. Jordán, "Incrementing bipartite digraph edge-connectivity", *Journal of Combinatorial Optimization*, 4(2000), 449-486.

[9] S. Gao, B. Novick and K. Qiu, "From Hall's matching theorem to optimal routing on hypercubes," *Journal of Combinatorial Theory (B)*, 74(1998), 291-301.

[10] S. Gao and D.F. Hsu, "Short containers in Cayley graphs," DIMACS Tech Report 2001-18, May 2001. (Available at http://www.math.clemson.edu/~sgao/pub.html).

[11] C. Godsil, "Connectivity of minimal Cayley graphs", *Arch. Math.*, 37(1981), 473-476.

[12] C. Godsil and G. Royle, *Algebraic Graph Theory*, Springer-Verlag New York, Inc., Graduate Texts in Mathematics, 2001.

[13] Y.O. Hamidoune, "Sur les atomes d'un graph orienté", *Comptes Rendus Academie des Sciences, Series A*, 284(1977), no.20, 1253-1256.

[14] Y.O. Hamidoune, "On the connectivity of Cayley digraphs", *European Journal of Combinatorics*, 5(1984), 309-312.

[15] Y.O. Hamidoune, A.S. Lladó and O. Serra, "The connectivity of hierarchical Cayley digraphs", *Discrete Applied Mathematics*, 37/38(1992), 275-280.

[16] Y.O. Hamidoune, A.S. Lladó and O. Serra, "Small cutsets in quasiminimal Cayley graphs", *Discrete Mathematics*, 159 (1996), 131-142.
[17] P.-S. Loh and L.J. Schulman, "Improved expansion of random Cayley graphs", *Discrete Mathematics and Theoretical Computer Science*, 6(2004), 523-528.
[18] A. Lubotzky, "Cayley graphs: Eigenvalues, expanders and random walks", in *Survey in Combinatorics 1995* (Ed., P. Rowlinson) Cambridge University Press, 1995, 155-189.
[19] J. Morris, "Connectivity of Cayley graphs: A special family", *The Journal of Combinatorial Mathematics and Combinatorial Computing*, 20, (1996), 111-120.
[20] P.S. Novikov, On the algorithmic unsolvability of the word problem in group theory. *Trudy Mat. Inst. im. Steklov*, 44. Izdat. Akad. Nauk SSSR, Moscow, 1955, 143 pp. (in Russian)
[21] S.T. Schibell and R.M. Stafford, "Processor interconnection networks from Cayley graphs", *Discrete Mathematics*, 40(1992), 333-357.
[22] M. Watkins, "Connectivity of transitive graphs", *Journal of Combinatorial Theory*, 8 (1970), 23-29.

Department of Mathematical Sciences, Clemson University, Clemson, SC, USA 29634-0975 *E-mail address*: SGAO, NBETH@CES.CLEMSON.EDU