Construction of Edge Fault-Tolerant Codes for Minimal Gossip Schemes

Suren, Poghosyan
Institute for Informatics and Automation Problems of NAS RA
Yerevan, Armenia
e-mail: psuren55@yandex.ru

Yeghisabet, Alaverdyan
National Polytechnic University of Armenia
Yerevan, Armenia
e-mail: ealaverdjan@gmail.com

ABSTRACT
The gossip problem, also the k-fault-tolerant gossiping, where at most k arbitrary faults of calls are allowed, is investigated. It is shown that for providing the stability of fault-tolerant gossip scheme, an application of some well designed error detection/correction technique is implied to address the failures specific to information dissemination. The fault-tolerant code introduced is based on edge redundancy, meanwhile the method underlying the construction of robust k-fault-tolerant gossiping exploits peculiarities of hypercube expander graphs. Efficiency of the construction is also considered.

Keywords
Gossip, fault-tolerant gossiping, edge redundancy, hy-percube, expander graph

1. INTRODUCTION
Robustness and stability are desired properties for any distributed computing environment, and thus for any communication system, where nodes represent processors, and edges represent communication links between the nodes. One of the major problems in the design of multi component systems is the presence of faults, and thus, the development of efficient techniques for fault handling is of a practical importance. Meanwhile, the fault tolerance is achieved through some degree of redundancy introduced specifically to address the given communication problem. The gossip problem, first proposed by Boyd, and also known as a telephone problem, concerns the information dissemination, where each of n nodes of a communication network has a unique piece of information that must be transmitted to all the other nodes using two-party telephone calls initiated to exchange every piece of information available at the time of the call. By the end, every node gets everyone else's information with a restriction that no node receives own piece of information from another node. A k-fault - tolerant graph is a multi graph with linearly ordered edges such that for any ordered pair of vertices u and v, there are $k+1$ edge-disjoint ascending paths from u to v.
The gossiping problem is to find the minimum number of calls achieving the information dissemination, and can be modeled by an ordered graph G, where each vertex (respectively, edge) corresponds to a unique party (respectively, telephone call), and edge-ordering indicates the ordering of two-party telephone calls. A vertex v receives the message originated from a vertex u if and only if there is an ascending path from u to v in the ordered graph G. The gossiping for n communicating parties is modeled by a corresponding gossip graph over n vertices. The minimum number of calls for n parties (respectively, nodes) was determined earlier to be $2n-4$ [1, 2, 3, 4], then certain improvements of the upper bounds were introduced in [5, 6].
Let $\tau\ (n,k)$ denotes the minimum number of edges in a k-fault tolerant gossip graph with n vertices. T. Hasunuma and H. Nagamochi [7] proved that the upper bound on the calls,

$$\tau(n,k) \leq \frac{1}{2}nk + O(n\ \log n). \tag{1}$$

Construction of k-fault-tolerant gossip scheme based on Wheel graph [8] represents a further improvement of the upper bound:

$$\tau(n,k) \leq \frac{2}{3}nk + O(n\ \log n) \tag{2}$$

for general n and k.

2. MATHEMATICAL PRELIMINARIES
The construction of an error detection/correction code for a robust k-fault tolerant gossip scheme involves techniques for tolerating edge fault (missed calls) in gossip graphs based on adding a definite number of redundant edges. This provides maintenance of the underlying binary relation of the original graph in the presence of edge faults. Meanwhile, edge redundancy is realized through involvement of an appropriate expander graph motivating the selection by the circumstance that mathematical apparatus of expander graphs [9] are well studied and approved. For the whole family of expanders every predefined set of vertices has many neighbors, and this very circumstance makes it possible to design a suitable error detection/correction technique.
In this model the architecture is viewed as a graph, where the nodes represent the processors and the edges represent communication links between the nodes. A target gossip graph G(V,E), where V is the set of vertices, and E is the set of edges, is selected and the required amount of fault tolerance, f, is determined. Then a fault tolerant graph $G'(V' \supset V,\ E' \supset E)$ is defined with the property that given any set of f or fewer faulty edges, the remaining graph, after removal of the faulty edges, is guaranteed to contain the target graph as a subgraph. Note that this approach guarantees that any algorithm designed for the target graph will run with no slowdown in the presence of f or fewer edge faults in the fault tolerant graph, regardless of their distribution. Minimizing the cost in this model amounts to

constructing a fault tolerant graph with minimum degree. Thus, construction of fault tolerant gossip graph is equivalent to the construction of a generator matrix for error detection/correction codes.
Fault-tolerant model is developed by using a d-dimensional hypercube network consisted of 2^d nodes encoded with d-bit binary codewords. Each node has d neighbors. For the purpose, the expander hypercube code is parameterized by a fixed-size code C for the regular expander graph G_d with constant degree d. The degree of the expander dictates uniform encoding and fixed-size length for the codewords, equal to d. The rate and distance of the new code depend on the rate and distance of C. If the Hamming distance of any two codewords of a code $C \geq d_{min}$, the code is said to have minimum distance d_{min}. The error detection and correction properties of a code are determined in part of its minimum distance. For a given d_{min},at least d_{min} errors are needed to transform a valid codeword to another. If there are fewer than d_{min} errors, the received invalid codeword is detected, then the latter is compared to all the valid codewords in the codebook to find the closest valid codeword to replace with. This makes it possible to deduce the original codeword, and thus the error correction can be achieved. The relative distance, denoted by δ, is the ratio of the distance to the codewords' block length, i.e. $\delta = d_{min}/n$.
Generally, a code provides t error correction and s additional error detection if and only if the following inequality holds.

$$2t + s + 1 \leq d_{min}. \tag{3}$$

The equation (3) suggests that a single error detection code, for which $s = 1$, $t = 0$, requires a $d_{min} = 2$, as for single parity check codes. A single error correction code, for which $s = 0$, $t = 1$, requires a $d_{min} = 3$, and a code with both single error correction and 2 more errors detection, for which $s = t = 1$, requires a minimum distance of 4.
The error detection and correction capabilities of a code are conditioned by the number of check bits and how the check bits are distributed over the information bits, not necessarily to be uniform. A good error detection/correction capability for a code suggests partial overlapping of information bits, which, particularly, may be obtained through application of m-out-of n codes. Concerned with algorithmic realization of the code, positioning the check bits may be in powers of two positions, or allocated to the left/right in the codeword. For n number of bits for a codeword and k check bits, the code rate is k/n.

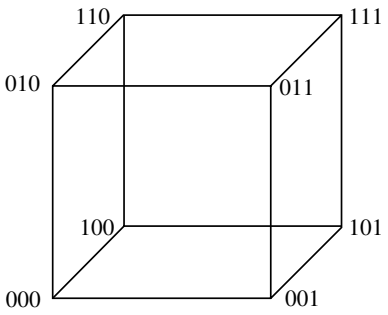

Figure 1. Hypercube expander

For the hypercube above, the codebook contains only 2 valid codewords, namely, 000 and 111. The other six invalid codewords are deduced to the closest valid codewords, thus correcting the error. Three changed bits between the valid codewords results in hamming distance of 3. For the hypercube, $d_{min} = d$, the fixed-size length of the codewords is also d.
Construction of error detection/correction code implies the following steps:
• The codewords' length is determined to be nd, where n is the number of the expander vertices, d is the degree of vertices, equal to d_{min} of the code.
•Edges are enumerated according to gossiping preferences
•The decimal value of the edge number flips the appropriate bit in the codeword bitstring to one.
• Cutson the expander may also be encoded, flipping the cut frame edge indicators to one.

The expander code construction due to Zemor [10] uses the fixed size code C of block length d and an expander gaph G on n vertices and degree d into a new code $Z = Z(C, G)$ with block length nd. The rate and the distance of the new code Z depend on rate and distance r and d_{min} of C, and on the spectral expansion λ of G. The hypercube expander $HE(C, G)$ is constructed to be a supergraph for the original gossip graph G endowed with n vertices and predefined set of edges, each of nd bit of length, as the newly constructed $HE(C, G)$ graph has nd number of edges. Resultant HE is regular and has $2n$ number of vertices in left and right vertex sets L and R. For an edge $e \in E$ with end points u and v in V, both u_L in L to v_R in R and v_L in L to u_R in R are connected. This creates a d-regular $2n$-vertex bipartite graph G'. Since the graph G' is constructed from an original G with spectral expansion λ, the expander mixing lemma [10] can be applied to this graph. Thus, for all sets $S \subset L$ and $T \subset R$, we have that

$$|e(S,T) - d\frac{|S||T|}{n}| \leq \lambda d\sqrt{|S||T|}, \tag{4}$$

where $e(S, T)$ represents the number of edges between the sets S and T.
The codewords for the G' graph are dn bits long, and G' has dn edges. Each bit position in the codeword is associated with an edge in G'. Aiming maintenance of gossip networks' paradigms, we can assume that edges incident to a gossip vertex obey to some predefined ordering, and this ordering takes place even if the certain codeword x is corrupted or lost. Thus, $x \in \{0, 1\}^{nd}$ is a codeword, $e_1, e_2, , e_d$ are incident edges of the vertex v, therefore $x_v = (x_{e_1}, x_{e_2}, , x_{e_d}) \in \{0, 1\}^d$, and this association takes place even if x is corrupted by the channel.

Note that linearity of the code C implies the linearity of G'. For a C code with $[d, rd, \delta d] - code\ with\ rate\ \ r < 1/2$ and a d-regular expander with $\lambda < \delta$, the $Z(C, G)$ code is $[nd, (2r - 1)nd, \delta(\delta - \lambda)nd]$ code [11].
Decoding for the expander is a recursive procedure, meanwhile, all the calculations for a chosen vertex is fully localized, and can be parallelized in a multiprocessor system. Also, linearity of the construction ensures high efficiency of the resolution. Thus, for the received x_v codeword, local decoding for $Z(C, G)$ involves searching for the received codeword in C, if $x_v \notin C$, for each $v \in V_i$ to decode x_v to the nearest codeword in C while considering both left and right partitions L and R on the expander.

3. ROBUST GOSSIPING

Another important characteristic for a code is its decoding error probability, when the received codeword, applied the d_{min} criterion, is decoded/deduced incorrectly. Another failure that also should not be neglected, is that the number of errors exceeds d_{min}, and no deducing is possible to even select one or more closer codewords. The latter happens when more than two deduced vectors match to d_{min}, called as ambiguity in decoding. This case is referred to as decoding failure vs. decoding error. This points out to the need for involving additional techniques for error detection/correction exploiting not only the minimum distance parameter.

To address decoding failure, we propose an additional protective mechanism to detect and fix ambiguity in decoding: application of an efficient systematic code with code rate 1/2. For this purpose, a quasigroup $(Q, *, /, |)$ of order 2^d endowed with three non associative operations is proposed [12].

Error correction is performed by exploiting the orthogonal parastroph of the given quasigroup. As the elements of the quasigroup are closely correlated to each other, the latter provides diffusion of the error within the code block. This results in detection of the error on the stage of the quasigroup equipped correction code, then, on the higher level of decoding, the minimum distance bounded decoding will deduce the received erroneous codeword to a closest valid codeword. Let C be an (n, k) code over $GF(q)$ with minimum distance d, where q stands for the base of computation. We assume C is being used to correct t errors, where t is a fixed integer satisfying the equation (3). Quasigroup equipped robust gossip code construction is demonstrated for a bipartite regular expander with $|L| = |R| = 4$vertices. For the given bipartite graph $G_{4,4}$ partitioned to equivalence classes $\{\{1, 3, 5, 7\}, \{2, 4, 6, 8\}\}$, a quasigroup of order 8 can be generated as follows:

Table 1. A quasigroup of order 8

*	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	1	2
3	5	6	7	8	1	2	3	4
4	7	8	1	2	3	4	5	6
5	8	7	6	5	4	3	2	1
6	2	1	4	3	6	5	8	7
7	4	3	8	7	2	1	6	5
8	6	3	2	1	8	7	4	3

The code using a quasigroup so generated will exploit the operation $*$ (the Cayley table of the quasigroup) over the codewords derived for the expander. In order to fix ambiguity in decoding, we extend the input message $a_1\ a_2\ a_3\ ...\ a_n$ to the block $a_1\ a_2\ a_3\ ...\ a_n\ d_1\ d_2\ d_3\ ...\ d_n$, where $d_i = a_i * a_{i+1} mod n, i = 1, 2, 3, ..., n$.

4. CONCLUSION

The code designed exploits the well-known characteristics of linear codes and expanders. From the whole family of expanders, the hypercube model is selected which exhibits all the essential properties of gossip graphs, meanwhile the fault-tolerant code is constructed based on the Zemor code. To address ambiguity problem specific to minimum distance codes, an additional systematic encoding/decoding based on orthogonal quasigroups is involved.

REFERENCES

[1] B. Baker and R. Shostak, "Gossips and telephones", Discrete Math, pp.191-193, 1972.

[2] R. Bumby, "A problem with telephones", Discrete Math, pp.13-18, 1981.

[3] A. Hajnal, E. Milner and E. Szemeredi, "A cure for the telephone disease", Canad. Math. Bull, pp. 447-450, 1976.

[4] R. Tijdeman, "On a telephone problem", Nieuw Arch. Wisk, pp. 188-192, 1971.

[5] A. Seress, "Quick gossiping by conference calls", Discrete Math, pp. 109-120, 1988.

[6] D. West, "Gossiping without duplicate transmissions", Discrete Math, pp. 418-419, 1982.

[7] T. Hasunuma, H. Nagamochi. "Improved bounds for minimum fault-tolerant gossip graphs", WG'11 Proceedings of the 37th international conference on Graph-Theoretic Concepts in Computer Science, 203- 214, 2011.

[8] V. Hovnanyan, S. Poghosyan, V. Pogosyan, "Fault-tolerant Gossip Graphs Based on Wheel Graphs", Mathematical Problems of Computer Science, pp. 42- 43, 2014.

[9] M. Sipser and D. Spielman, "Expander codes", IEEE Transactions on Information Theory, pp. 1710-1722, 1996.

[10] A. Barg and G. Zemor, "Error Exponents of Expander Codes", IEEE Transactions on Information Theory, pp. 1725-1729, 2002.

[11] G. Zemor, "On Expander Codes", IEEE Transactions on Information Theory, pp. 835-837, 2001.

[12] Y. Alaverdyan, "Graph Based Orthogonal Quasigroups in Design of Error-Correcting Codes", Annual Session of Armenian Mathematical union devoted to 90- aniv. Of Rafael Alexandryan, pp. 13-14, 2013.