Mathematical Problems of Computer Science 38, 74–75, 2012.

Partition and Coloring in Design of Quasigroup Equipped Error-detecting Codes

G. Margarov, Y. Alaverdyan

State Engineering University in Armenia
gmargarov@gmail.com, ealaverdjan@gmail.com

Nowadays advances in communications and coding theory result in new coding concepts reinforced with more efficient data structures, such as codes on graphs. Classes of equivalencies on graphs generating a special class of permutations, so called cycles, may be a research area of great current interest beside low-density parity check (LDPC) codes and turbo codes. In this paper graph partition and coloring based generation of quasigroups for designing error-detection codes is proposed. The method makes it possible to introduce a class of codes, generated by quasigroup string transformations, which are efficient and almost random.

Let A denote the finite set of a graph with n vertices, and S_n is a group of permutations on the set A containing $n!$ number of distinct permutations. Let the series of 1, 2, ..., n denotes the elements of A and a binary relation R on the set A, aRb, be defined for a fixed permutation σ if $b = \sigma^k(a)$ for a nonnegative integer k. Obviously, R presents an equivalence relation.

As R is a relation of equivalency, it partitions the set A into classes of equivalency. For example, let $A = 1, 2, 3, 4, 5, 6, 7, 8$ presents the set of vertices of some simple graph and

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 7 & 8 & 6 & 1 & 5 \end{pmatrix}.$$

Obviously, the set of classes of equivalency is $\{\{1, 4, 7\}, \{2, 3\}, \{5, 8\}, \{6\}\}$ according to reflexivity, symmetry and transitivity of ordered pairs in the relation. The set of classes of equivalency is called also the orbit of the permutation S_n. An elementary class of such a relation may be introduced on the basis of bipartite graphs which are bichromatic. Such a coloring partitions the given graph into two non intersected subsets of vertices. To design an error-detection code and a quasigroup of an appropriate order, a special class of permutation, a cycle, is introduced as follows: $\sigma_c = (a_1, a_2, a_3, ..., a_k)$ is a cycle, where $\sigma_c(a_i) = a_{i+1}$ for $i < k$ and $\sigma_c(a_k) = a_1$. For example, if $\sigma_c = (1, 4, 6, 8)$ is a cycle in S_8, then

$$\sigma_c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 3 & 6 & 5 & 8 & 7 & 1 \end{pmatrix}. \quad (1)$$

The permutation given in (1) may be presented as a product of cycles, which have no common elements. For that purpose, firstly, the set A is partitioned to classes of equivalency. Then we choose an element a and form a cycle as follows: $(a, \sigma(a), \sigma^2(a), \sigma^3(a), ..., \sigma^k(a))$,

where $\sigma^{k+1} = a$. These cycles do not contain common elements, as classes of equivalencies do not intersect. Each element in a class moves only the items in the given cycle. Even more, the order of cycles doesn't affect the permutation so designed. Cycles with one element also do not alter the permutation and are subject to further investigation, as they have to be tested for capability to detect errors.

Cycles stand for a good structural background to design quasigroups of appropriate order. For the given bipartite graph $G_{4,4}$ partitioned to 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 permutations over finite sets are closed and associative with respect to the binary operation of composition. Therefore, the set of all the permutations over a fixed finite sets forms a group over the operation of composition. Thus, the composition of the two given permutations results in new permutations and cycles and introduces new classes of equivalency. For example, given two cycles, $\sigma = \{\{1, 3, 4\}, \{2, 5\}\}$ and $\tau = \{\{1, 2\}, \{3, 4\}, \{5\}\}$,their composition is as follows:

$$\sigma \circ \tau = \{\{1, 5, 2, 3\}, \{4\}\}.$$

This, in turn, points out to the possibility of not only inverting, but also factoring permutations by designing a homomorphism. Given $(G, \bullet)$ and $(H, *)$, where $\bullet$ and $*$ are operations over groups G and H respectively, $f : G \longrightarrow H$ is a homomorphism, if $f(g \bullet g') = f(g) * f(g')$ for all g, g' in G. Depending on the type of the function f, we derive particular types of homomorphism. Error-detection codes using quasigroups so generated, will exploit the quasigroup operation $*$ on the set A. In order to detect errors, we extend the input message $a_1\ a_2\ a_3\ \ldots\ a_n$ to block $a_1\ a_2\ a_3\ \ldots\ a_n\ d_1\ d_2\ d_3\ \ldots\ d_n$, where $d_i = a_i * a_{i+1} \bmod n$, $i = 1, 2, 3, \ldots, n$. A future work will be dedicated to assessment of efficiency of the proposed method versus existing resolutions.

References

[1] Yu.M. Movsisyan, *Hyperidentities in algebras and varieties*, Uspekhi Matematicheskikh Nauk, Vol.53, No. 1(319), 61–114, 1998. English translation in Russian Mathematical Surveys 53, 1 , 57–108, 1998.

[2] I. Anderson, *A first course in discrete mathematics*, Springer-Verlag, London, 2001.

[3] J. Cooper, D. Donovan and J. Seberry, *Secret sharing schemes arising from Latin squares*, Bull. Inst. Combin. Appl., 12, 1994, 33-43.