Performance of ReedSolomon codes using the GuruswamiSudan algorithm with improved interpolation efficiency

Kwame Ackah Bohulu

January 17, 2019

1 Groups

A group is defined as a set **G** with an operation Δ which is associative (i.e $(a\Delta b)\Delta c = a\Delta(b\Delta c)$) has a neutral elements and each element has an inverse. Below is a formal definition

Definition: A set **G** is called a group if it satisfies the ff axioms

- operation Δ is associative (i.e $(a\Delta b)\Delta c = a\Delta(b\Delta c)$)
- There exists an element e in G such that $a\Delta e = e\Delta a = a$ for every a in **G**
- For every element a in G, there is an element a^{-1} in G such that $a\Delta a^{-1} = a^{-1}\Delta a = e$

  The symbol used to represent a group is $< \mathbf{G}, \Delta >$

  Groups are important because they serve as a foundation from which more complex algebraic structures can be created. In many scientific applications, finite groups are highly important because in most real world applications a finite number of objects is dealt with

  If the commutative law $(a\Delta b = b\Delta a)$ holds in a group, it is known as an Abelian group.

  Examples of groups include the additive group of integers$(< \mathbb{Z}, + >)$, additive group of rational numbers $(< \mathbb{Q}, + >)$and the additive group of real numbers $(< \mathbb{R}, + >)$

2 Elementary properties of Groups

Below are a few elementary properties of Groups

- Every group has exactly one identity element and one inverse element
- For additive groups, the identity element is 0 and the inverse of a is $-a$
- For multiplicative groups, the identity element is 1 and the inverse of a is a^{-1}

The most basic rule of group-related calculations is the cancellation rule given by the theorem below

Theorem 1: if **G** is a group and a, b, c are elements of **G**,then

- $ab = ac$ implies $b = c$ and
- $ba = ca$ implies $b = c$

To prove Theorem 1, multiply the respective equations a^{-1}

Theorem 2: if **G** is a group and a, b are elements of **G**,then

$$ab = e \text{ implies } a = b^{-1}$$

and

$$ba = e \text{ implies } b = a^{-1}$$

To proove Theorem 2 use the fact that $aa^{-1} = bb^{-1} = e$

The next theorem gives useful information related to how to calculate inverses

Theorem 3: if **G** is a group and a, b are elements of **G**,then

- $(ab)^{-1} = b^{-1}a^{-1}$
- $(a^{-1})^{-1} = a$

If **G** is a finite group, the number of elements in **G** is called the order of **G** and is written as $|G|$

2.1 Subgroups

Definition: Let G be a group and S a nonempty subset of G. If S is closed with respect to opetation Δ and closed with respect to inverses S is a subgroup of G.

An example is the set of all even integers which is a subgroup of the additive group of integers $\mathbb{Z}$ From henceforth, we will use the set symbol to represent the group and assume that the operation that is being used in the group is multiplication. It is worth noting that if S is a subgroup of G, the operations on S and G are the same. Additionally, if G is a group and S is its subgroup, S is also a group.

Subgroups are useful given the fact that they can be used to show that certain things are groups. The smallest and largest possible subgroups of a group G are the one-element subgroup that contains the identity element e and the group G itself respectively. These groups are known as trivial subgroups, whiles every other subgroup is known as a proper subgroup.

Now, assuming group G has elements a, b, c it is possible to define a subgroup S made up of all product combinations of a, b, c and their inverses a^{-1}, b^{-1}, c^{-1}. In such a situation, we refer to S as the subgroup of G generated by a, b, c. It is also possible to generate a finite subgroup of n elements S from a single element a in G using the previous methodology. A subgroup S generated in such a way is known as a *cyclic subgroup*. Cyclic groups are denoted by $< a >$ and a is called the *generator* of S. It is worth noting that $< a >$ contains all possible products of a and a^{-1} By extension, a cyclic group G is a generated by a single element a