When does a product of group elements equal its reverse?

Joseph Rower

California Lutheran University

May 15, 2008

Commutativity

- $3 \cdot 5 = 15 = 5 \cdot 3$
- But does ab=ba in all cases??
- Of course not, then math would be simple...
- Commutativity holds true for integers but not matrices

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 16 & 17 \end{pmatrix}$$

which doesn't equal

$$\begin{pmatrix} 13 & 20 \\ 7 & 10 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Commutativity

- $3 \cdot 5 = 15 = 5 \cdot 3$
- But does ab=ba in all cases??
- Of course not, then math would be simple...
- Commutativity holds true for integers but not matrices

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 16 & 17 \end{pmatrix}$$

which doesn't equal

$$\begin{pmatrix} 13 & 20 \\ 7 & 10 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Commutativity

- $3 \cdot 5 = 15 = 5 \cdot 3$
- But does ab=ba in all cases??
- Of course not, then math would be simple...
- Commutativity holds true for integers but not matrices

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 16 & 17 \end{pmatrix}$$

which doesn't equal

$$\begin{pmatrix} 13 & 20 \\ 7 & 10 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Commutativity

- $3 \cdot 5 = 15 = 5 \cdot 3$
- But does ab=ba in all cases??
- Of course not, then math would be simple...
- Commutativity holds true for integers but not matrices

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 7 \\ 16 & 17 \end{pmatrix}$$

which doesn't equal

$$\begin{pmatrix} 13 & 20 \\ 7 & 10 \end{pmatrix} = \begin{pmatrix} 4 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

So when does $ab = ba$?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.

So when does $ab = ba$?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.

So when does $ab = ba$?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.

Definition

Let G be a nonempty set with a *binary operation*. G is a group if the following properties are satisfied.

CLOSURE

The binary operation assigns every ordered pair (a, b) where $a, b \in G$ to a result ab with $ab \in G$.

ASSOCIATIVITY

The operation is associative; that is, $ab(c) = a(bc)$ for all $a, b, c \in G$.

IDENTITY

There is an element e (called the *identity*) in G such that $ae = ea = a$ for all $a \in G$.

INVERSES

For each $a \in G$, there is an element $b \in G$ (called the *inverse* of a) such that $ab = ba = e$.

So when does $ab = ba$?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.

Groups

1. Integers under addition
2. Reals (not including 0) under multiplication
3. Invertible n by n matrices with real entries

Not Groups

1. Reals (including 0) under multiplication
2. Integers under multiplication (no inverses)

So when does ab=ba?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.
- To make this problem interesting the group needs to be non-Abelian.

So when does ab=ba?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.
- To make this problem interesting the group needs to be non-Abelian.

Definition

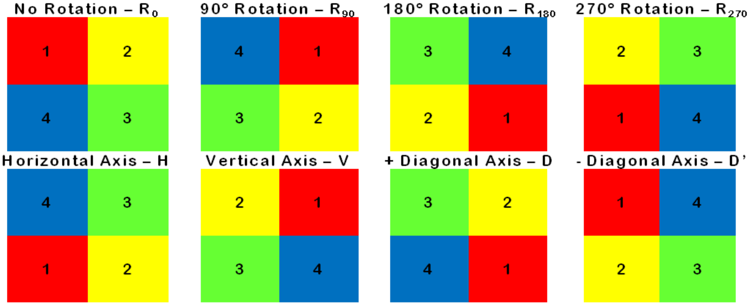
A group is *Abelian* if $ab = ba$ for every pair of elements a and b.

So when does ab=ba?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.
- To make this problem interesting the group needs to be non-Abelian.
- We'll limit ourselves to finite groups.

So when does ab=ba?

- To answer this question, we need a little preliminary information:
- First off, I have to be in a group.
- To make this problem interesting the group needs to be non-Abelian.
- We'll limit ourselves to finite groups.
- A great example of a finite, non-Abelian group is $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.



What's so great about D_4?

We can multiply elements in D_4, for example $R_{90} \cdot H$

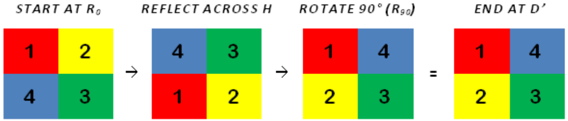


Figure: Multiplication in D_4

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D'	V	R_{90}	R_{270}	R_{180}	R_0

Commutation in D_4

- Some of these products commute, for example $R_{180} \cdot H = V = H \cdot R_{180}$

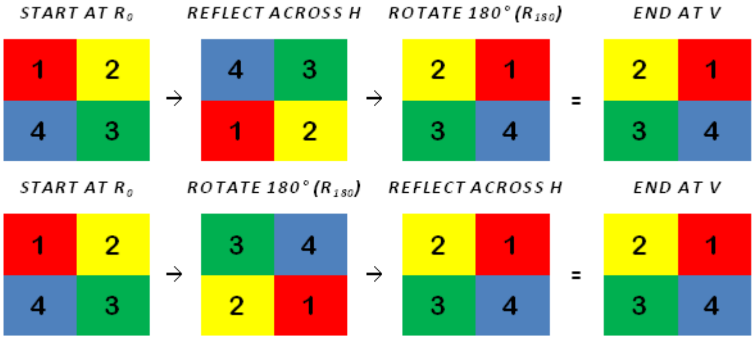


Figure: Commuting Product in D_4

Commutation in D_4

- Some of these products commute, for example $R_{180} \cdot H = V = H \cdot R_{180}$
- So how many two element pairs commute in D_4?
- What is the probability that two elements commute in D_4?
- What is the maximum probability that two elements in any non-Abelian finite group G commute?

Definition

A product of n elements is reversibly commutative if the product $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$.

Commutation in D_4

- Some of these products commute, for example $R_{180} \cdot H = V = H \cdot R_{180}$
- So how many two element pairs commute in D_4?
- What is the probability that two elements commute in D_4?
- What is the maximum probability that two elements in any non-Abelian finite group G commute?

Definition

A product of n elements is reversibly commutative if the product $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$.

Commutation in D_4

- Some of these products commute, for example $R_{180} \cdot H = V = H \cdot R_{180}$
- So how many two element pairs commute in D_4?
- What is the probability that two elements commute in D_4?
- What is the maximum probability that two elements in any non-Abelian finite group G commute?

Definition

A product of n elements is reversibly commutative if the product $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$.

Commutation in D_4

- Some of these products commute, for example $R_{180} \cdot H = V = H \cdot R_{180}$
- So how many two element pairs commute in D_4?
- What is the probability that two elements commute in D_4?
- What is the maximum probability that two elements in any non-Abelian finite group G commute?

Definition

A product of n elements is reversibly commutative if the product $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$.

Commutation in D_4

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	1	1	1	1	1	1	1	1
R_{90}	1	1	1	1	0	0	0	0
R_{180}	1	1	1	1	1	1	1	1
R_{270}	1	1	1	1	0	0	0	0
H	1	0	1	0	1	1	0	0
V	1	0	1	0	1	1	0	0
D	1	0	1	0	0	0	1	1
D'	1	0	1	0	0	0	1	1

- The 1's in the table represent a product that commutes.
- The sum of the 1's in the table is then the total number of commuting pairs.
- Turns out there are 40 1's in that table...and 64 total squares.
- So it makes sense that the probability of the product of two elements commuting in D_4 is $\frac{40}{64}$ or $\frac{5}{8}$.

Commutation in D_4

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	1	1	1	1	1	1	1	1
R_{90}	1	1	1	1	0	0	0	0
R_{180}	1	1	1	1	1	1	1	1
R_{270}	1	1	1	1	0	0	0	0
H	1	0	1	0	1	1	0	0
V	1	0	1	0	1	1	0	0
D	1	0	1	0	0	0	1	1
D'	1	0	1	0	0	0	1	1

- The 1's in the table represent a product that commutes.
- The sum of the 1's in the table is then the total number of commuting pairs.
- Turns out there are 40 1's in that table...and 64 total squares.
- So it makes sense that the probability of the product of two elements commuting in D_4 is $\frac{40}{64}$ or $\frac{5}{8}$.

Commutation in D_4

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	1	1	1	1	1	1	1	1
R_{90}	1	1	1	1	0	0	0	0
R_{180}	1	1	1	1	1	1	1	1
R_{270}	1	1	1	1	0	0	0	0
H	1	0	1	0	1	1	0	0
V	1	0	1	0	1	1	0	0
D	1	0	1	0	0	0	1	1
D'	1	0	1	0	0	0	1	1

- The 1's in the table represent a product that commutes.
- The sum of the 1's in the table is then the total number of commuting pairs.
- Turns out there are 40 1's in that table...and 64 total squares.
- So it makes sense that the probability of the product of two elements commuting in D_4 is $\frac{40}{64}$ or $\frac{5}{8}$.

Commutation in D_4

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	1	1	1	1	1	1	1	1
R_{90}	1	1	1	1	0	0	0	0
R_{180}	1	1	1	1	1	1	1	1
R_{270}	1	1	1	1	0	0	0	0
H	1	0	1	0	1	1	0	0
V	1	0	1	0	1	1	0	0
D	1	0	1	0	0	0	1	1
D'	1	0	1	0	0	0	1	1

- The 1's in the table represent a product that commutes.
- The sum of the 1's in the table is then the total number of commuting pairs.
- Turns out there are 40 1's in that table...and 64 total squares.
- So it makes sense that the probability of the product of two elements commuting in D_4 is $\frac{40}{64}$ or $\frac{5}{8}$.

What about a group G?

- What is the maximum probability that two elements in a group commute?
- An easy proof shows that $Pr(ab = ba) = \frac{5}{8}$.

  The proof depends on the *center* of a group, denoted $Z(G)$.

Definition

The *center* of a group G is the subset of elements in G that commute with every element of G. So $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$.

The bigger the *center* of a group is, the more element pairs will commute.

What about a group G?

- What is the maximum probability that two elements in a group commute?
- An easy proof shows that $Pr(ab = ba) = \frac{5}{8}$.

The proof depends on the *center* of a group, denoted $Z(G)$.

Definition

The *center* of a group G is the subset of elements in G that commute with every element of G. So $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$.

The bigger the *center* of a group is, the more element pairs will commute.

What about a group G?

- What is the maximum probability that two elements in a group commute?
- An easy proof shows that $Pr(ab = ba) = \frac{5}{8}$.

  The proof depends on the *center* of a group, denoted $Z(G)$.

Definition

The *center* of a group G is the subset of elements in G that commute with every element of G. So $Z(G) = \{a \in G \mid ax = xa \text{ for all } x \in G\}$.

The bigger the *center* of a group is, the more element pairs will commute.

What about a group G?

- What is the maximum probability that two elements in a group commute?
- An easy proof shows that $Pr(ab = ba) = \frac{5}{8}$.

  In D_4, $Z(G) = \{R_0; R_{180}\}$, as highlighted below.

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
R_{90}	**1**	1	**1**	1	0	0	0	0
R_{180}	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
R_{270}	**1**	1	**1**	1	0	0	0	0
H	**1**	0	**1**	0	1	1	0	0
V	**1**	0	**1**	0	1	1	0	0
D	**1**	0	**1**	0	0	0	1	1
D'	**1**	0	**1**	0	0	0	1	1

What about a group G?

- So what is the $max|Z(G)|$ in a non-Abelian group?
- Intuitively, we know that $|Z(G)| \leq |C(g \notin Z(G))| \leq |G|$.
- By Lagrange's Theorem we know that each partition is no more than $\frac{1}{2}$ the size of the preceding partition.
- This yields the result that $|Z(G)| \leq \frac{|G|}{4}$ for a non-Abelian group, and in fact $|Z(G)| = \frac{|G|}{4}$ for a group with maximal non-Abelian commutativity.

What about a group G?

- So what is the $max|Z(G)|$ in a non-Abelian group?
- Intuitively, we know that $|Z(G)| \leq |C(g \notin Z(G))| \leq |G|$.
- By Lagrange's Theorem we know that each partition is no more than $\frac{1}{2}$ the size of the preceding partition.
- This yields the result that $|Z(G)| \leq \frac{|G|}{4}$ for a non-Abelian group, and in fact $|Z(G)| = \frac{|G|}{4}$ for a group with maximal non-Abelian commutativity.

What about a group G?

- So what is the $max|Z(G)|$ in a non-Abelian group?
- Intuitively, we know that $|Z(G)| \leq |C(g \notin Z(G))| \leq |G|$.
- By Lagrange's Theorem we know that each partition is no more than $\frac{1}{2}$ the size of the preceding partition.
- This yields the result that $|Z(G)| \leq \frac{|G|}{4}$ for a non-Abelian group, and in fact $|Z(G)| = \frac{|G|}{4}$ for a group with maximal non-Abelian commutativity.

What about a group G?

- So what is the $max|Z(G)|$ in a non-Abelian group?
- Intuitively, we know that $|Z(G)| \leq |C(g \notin Z(G))| \leq |G|$.
- By Lagrange's Theorem we know that each partition is no more than $\frac{1}{2}$ the size of the preceding partition.
- This yields the result that $|Z(G)| \leq \frac{|G|}{4}$ for a non-Abelian group, and in fact $|Z(G)| = \frac{|G|}{4}$ for a group with maximal non-Abelian commutativity.

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Knowing that $|Z(G)| = \frac{|G|}{4}$ yields a great way to partition the group, into cosets of the center, labeled $gZ(G)$, of which there will be 4 for every group of maximal probability.
- For example, the cosets of D_4 are: $R_0 \cdot Z(G) = \{R_0, R_{180}\}$, $R_{90} \cdot Z(G) = \{R_{90}, R_{270}\}$, $H \cdot Z(G) = \{H, V\}$, and $D \cdot Z(G) = \{D, D'\}$.
- This gives structure to the problem, as we know several properties about multiplication in cosets. Given $g_1, g_2 \in gZ(G)$, $h \in hZ(G)$, $k \in kZ(G)$, and $z \in Z(G)$.

1. $g_1 \cdot g_2 \in Z(G)$
2. $g_1 \cdot h \in kZ(G)$
3. $g_1 \cdot h \cdot k \in Z(G)$
4. $g_1 \cdot z \in gZ(G)$

What about a group G?

- Another version of the proof provides a more general result, based on a group's conjugacy classes.

$$Pr(ab = ba) = \frac{k}{|G|}$$

where k is the number of conjugacy classes in the group G.

Definition

The *conjugacy class* of $g \in G$ is the set: $\{x^{-1}gx \mid x \in G\}$.
Conjugacy classes of D_4: $\{R_0\}$,$\{R_{180}\}$,$\{R_{90}, R_{270}\}$,$\{H, V\}$,$\{D, D'\}$

- So, since D_4 has 5 conjugacy classes and 8 elements:

$$Pr(ab = ba) = \frac{5}{8}$$

What about a group G?

- Another version of the proof provides a more general result, based on a group's conjugacy classes.

$$Pr(ab = ba) = \frac{k}{|G|}$$

where k is the number of conjugacy classes in the group G.

Definition

The *conjugacy class* of $g \in G$ is the set: $\{x^{-1}gx \mid x \in G\}$.
Conjugacy classes of D_4: $\{R_0\}$,$\{R_{180}\}$,$\{R_{90}, R_{270}\}$,$\{H, V\}$,$\{D, D'\}$

- So, since D_4 has 5 conjugacy classes and 8 elements:

$$Pr(ab = ba) = \frac{5}{8}$$

What about a group G?

- Another version of the proof provides a more general result, based on a group's conjugacy classes.

$$Pr(ab = ba) = \frac{k}{|G|}$$

where k is the number of conjugacy classes in the group G.

Definition

The *conjugacy class* of $g \in G$ is the set: $\{x^{-1}gx \mid x \in G\}$.
Conjugacy classes of D_4: $\{R_0\}$,$\{R_{180}\}$,$\{R_{90}, R_{270}\}$,$\{H, V\}$,$\{D, D'\}$

- So, since D_4 has 5 conjugacy classes and 8 elements:

$$Pr(ab = ba) = \frac{5}{8}$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

Reversible Commutativity

- Understanding the methods for finding the probability that a two element ordered pair commutes, can we extend them to a multiple element product?
- Computation by GAP software shows the following probabilities for reversible commutativity:

Products	maxPr(comm)
$ab = ba$ and $abc = cba$	$\frac{5}{8}$
$abcd = dcba$ and $abcde = edcba$	$\frac{17}{32}$
$abcdef = fedcba$ and $abcdefg = gfedcba$	$\frac{65}{128}$

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- We know that $maxPr(ab = ba) = \frac{5}{8}$.
- If we fix b in the product $abc = cba$ we can simplify the three element case as follows:

$$\begin{aligned} abc &= cba \\ xy &= ybxb^{-1} \\ xyb &= ybx \\ st &= ts \end{aligned}$$

- This says that no matter we choose as our b, there are $\frac{5}{8}|G|^2$ choices for (a, c) such that $abc = cba$.
- So we know why $maxPr(abc = cba) = \frac{5}{8}$.

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- We know that $maxPr(ab = ba) = \frac{5}{8}$.
- If we fix b in the product $abc = cba$ we can simplify the three element case as follows:

$$\begin{aligned} abc &= cba \\ xy &= ybxb^{-1} \\ xyb &= ybx \\ st &= ts \end{aligned}$$

- This says that no matter we choose as our b, there are $\frac{5}{8}|G|^2$ choices for (a, c) such that $abc = cba$.
- So we know why $maxPr(abc = cba) = \frac{5}{8}$.

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We know that $maxPr(ab = ba) = \frac{5}{8}$.
- If we fix b in the product $abc = cba$ we can simplify the three element case as follows:

$$\begin{aligned} abc &= cba \\ xy &= ybxb^{-1} \\ xyb &= ybx \\ st &= ts \end{aligned}$$

- This says that no matter we choose as our b, there are $\frac{5}{8}|G|^2$ choices for (a, c) such that $abc = cba$.
- So we know why $maxPr(abc = cba) = \frac{5}{8}$.

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We continue by fixing the middle elements (b, c) in the product $abcd = dcba$, which produces two possible cases.

  1. If $bc = cb = x$, then our product simplifies to $axd = dxa$, which we've shown to have solutions in $\frac{5}{8}|G|^2$ cases.
     - Since $maxPr(bc = cb) = \frac{5}{8}$, we see that this case accounts for $\frac{5}{8} \cdot \frac{5}{8}|G|^2 = \frac{25}{64}|G|^2$ of the commuting 4-tuplets.
  2. If $bc \neq cb$, then we can show that there are $\frac{3}{8}|G|^2$ possible choices for (a, d) so that $abcd = dcba$ is true.
     - Since $maxPr(bc \neq cb) = \frac{3}{8}$, we see that this case accounts for $\frac{3}{8} \cdot \frac{3}{8}|G|^2 = \frac{9}{64}|G|^2$ of the commuting 4-tuplets.

- Combining these two cases, we see that as expected:

$$maxPr(abcd = dcba) = \left(\frac{25}{64} + \frac{9}{64}\right) \cdot \frac{|G|^2}{|G|^2} = \frac{17}{32}$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We continue by fixing the middle elements (b, c) in the product $abcd = dcba$, which produces two possible cases.

1. If $bc = cb = x$, then our product simplifies to $axd = dxa$, which we've shown to have solutions in $\frac{5}{8}|G|^2$ cases.
   - Since $maxPr(bc = cb) = \frac{5}{8}$, we see that this case accounts for $\frac{5}{8} \cdot \frac{5}{8}|G|^2 = \frac{25}{64}|G|^2$ of the commuting 4-tuplets.
2. If $bc \neq cb$, then we can show that there are $\frac{3}{8}|G|^2$ possible choices for (a, d) so that $abcd = dcba$ is true.
   - Since $maxPr(bc \neq cb) = \frac{3}{8}$, we see that this case accounts for $\frac{3}{8} \cdot \frac{3}{8}|G|^2 = \frac{9}{64}|G|^2$ of the commuting 4-tuplets.

- Combining these two cases, we see that as expected:

$$maxPr(abcd = dcba) = \left(\frac{25}{64} + \frac{9}{64}\right) \cdot \frac{|G|^2}{|G|^2} = \frac{17}{32}$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We continue by fixing the middle elements (b, c) in the product $abcd = dcba$, which produces two possible cases.

  1. If $bc = cb = x$, then our product simplifies to $axd = dxa$, which we've shown to have solutions in $\frac{5}{8}|G|^2$ cases.
     - Since $maxPr(bc = cb) = \frac{5}{8}$, we see that this case accounts for $\frac{5}{8} \cdot \frac{5}{8}|G|^2 = \frac{25}{64}|G|^2$ of the commuting 4-tuplets.
  2. If $bc \neq cb$, then we can show that there are $\frac{3}{8}|G|^2$ possible choices for (a, d) so that $abcd = dcba$ is true.
     - Since $maxPr(bc \neq cb) = \frac{3}{8}$, we see that this case accounts for $\frac{3}{8} \cdot \frac{3}{8}|G|^2 = \frac{9}{64}|G|^2$ of the commuting 4-tuplets.

- Combining these two cases, we see that as expected:

$$maxPr(abcd = dcba) = \left(\frac{25}{64} + \frac{9}{64}\right) \cdot \frac{|G|^2}{|G|^2} = \frac{17}{32}$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We continue by fixing the middle elements (b, c) in the product $abcd = dcba$, which produces two possible cases.
  1. If $bc = cb = x$, then our product simplifies to $axd = dxa$, which we've shown to have solutions in $\frac{5}{8}|G|^2$ cases.
     - Since $maxPr(bc = cb) = \frac{5}{8}$, we see that this case accounts for $\frac{5}{8} \cdot \frac{5}{8}|G|^2 = \frac{25}{64}|G|^2$ of the commuting 4-tuplets.
  2. If $bc \neq cb$, then we can show that there are $\frac{3}{8}|G|^2$ possible choices for (a, d) so that $abcd = dcba$ is true.
     - Since $maxPr(bc \neq cb) = \frac{3}{8}$, we see that this case accounts for $\frac{3}{8} \cdot \frac{3}{8}|G|^2 = \frac{9}{64}|G|^2$ of the commuting 4-tuplets.
- Combining these two cases, we see that as expected:

$$maxPr(abcd = dcba) = \left(\frac{25}{64} + \frac{9}{64}\right) \cdot \frac{|G|^2}{|G|^2} = \frac{17}{32}$$

Finding $maxPr(a_1a_2 \cdots a_n = a_n \cdots a_2a_1)$

- How can we generalize these results to find the $maxPr(a_1a_2 \cdots a_{n-1}a_n = a_na_{n-1} \cdots a_2a_1)$?
- By fixing the middle elements $x_1 = a_2 \cdots a_{n-1}$ and $x_2 = a_{n-1} \cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1a_2 \cdots a_n = a_n \cdots a_2a_1$ simplifies to the case $a_1xa_n = a_nxa_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1x_1a_n = a_nx_2a_1) = \frac{3}{8}$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1x_2^{-1} = a_1a_na_1^{-1}a_n^{-1} \neq e$, which implies that $a_1a_n \neq a_na_1$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
   - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- How can we generalize these results to find the $maxPr(a_1a_2\cdots a_{n-1}a_n = a_na_{n-1}\cdots a_2a_1)$?
- By fixing the middle elements $x_1 = a_2\cdots a_{n-1}$ and $x_2 = a_{n-1}\cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1a_2\cdots a_n = a_n\cdots a_2a_1$ simplifies to the case $a_1xa_n = a_nxa_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1x_1a_n = a_nx_2a_1) = \frac{3}{8}$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1x_2^{-1} = a_1a_na_1^{-1}a_n^{-1} \neq e$, which implies that $a_1a_n \neq a_na_1$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
   - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- How can we generalize these results to find the $maxPr(a_1a_2\cdots a_{n-1}a_n = a_na_{n-1}\cdots a_2a_1)$?
- By fixing the middle elements $x_1 = a_2\cdots a_{n-1}$ and $x_2 = a_{n-1}\cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1a_2\cdots a_n = a_n\cdots a_2a_1$ simplifies to the case $a_1xa_n = a_nxa_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1x_1a_n = a_nx_2a_1) = \frac{3}{8}$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1x_2^{-1} = a_1a_na_1^{-1}a_n^{-1} \neq e$, which implies that $a_1a_n \neq a_na_1$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
   - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- How can we generalize these results to find the $maxPr(a_1 a_2 \cdots a_{n-1} a_n = a_n a_{n-1} \cdots a_2 a_1)$?
- By fixing the middle elements $x_1 = a_2 \cdots a_{n-1}$ and $x_2 = a_{n-1} \cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$ simplifies to the case $a_1 x a_n = a_n x a_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1 x_1 a_n = a_n x_2 a_1) = \frac{3}{8}$.
    - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1 x_2^{-1} = a_1 a_n a_1^{-1} a_n^{-1} \neq e$, which implies that $a_1 a_n \neq a_n a_1$.
    - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
    - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- How can we generalize these results to find the $maxPr(a_1a_2\cdots a_{n-1}a_n = a_na_{n-1}\cdots a_2a_1)$?
- By fixing the middle elements $x_1 = a_2\cdots a_{n-1}$ and $x_2 = a_{n-1}\cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1a_2\cdots a_n = a_n\cdots a_2a_1$ simplifies to the case $a_1xa_n = a_nxa_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1x_1a_n = a_nx_2a_1) = \frac{3}{8}$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1x_2^{-1} = a_1a_na_1^{-1}a_n^{-1} \neq e$, which implies that $a_1a_n \neq a_na_1$.
   - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
   - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- How can we generalize these results to find the $maxPr(a_1a_2\cdots a_{n-1}a_n = a_na_{n-1}\cdots a_2a_1)$?
- By fixing the middle elements $x_1 = a_2\cdots a_{n-1}$ and $x_2 = a_{n-1}\cdots a_2$, we can break our product into one of two cases.

1. If $x_1 = x_2 = x$, then $a_1a_2\cdots a_n = a_n\cdots a_2a_1$ simplifies to the case $a_1xa_n = a_nxa_1$, which has $maxPr = \frac{5}{8}$.
2. If $x_1 \neq x_2$, then we can show that $maxPr(a_1x_1a_n = a_nx_2a_1) = \frac{3}{8}$.
    - When $x_1 \neq x_2$, and $x_1, x_2 \in Z(G)$, then our product can be rearranged to the form $x_1x_2^{-1} = a_1a_na_1^{-1}a_n^{-1} \neq e$, which implies that $a_1a_n \neq a_na_1$.
    - When $x_1 \neq x_2$, and $x_1, x_2 \notin Z(G)$, we find that solutions only occur when $x_1 \in cl(x_2)$.
    - Both of these cases give $\frac{3}{8}|G|^2$ possibilities for (a_1, a_n).

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- If $x_1 = x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{5}{8}$.
- We know $Pr(x_1 = x_2)$ is the same probability as a product with one less transposition.

- If $x_1 \neq x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{3}{8}$.
- This will happen with $Pr(y_1 \neq y_2) = 1 - Pr(x_1 = x_2)$.

- Combining these yield the following probability formula:

$$maxPr(a_1 x_1 a_n = a_n x_2 a_1) = \frac{5}{8} \cdot Pr(x_1 = x_2) + \frac{3}{8} \cdot (1 - Pr(x_1 = x_2))$$

- Is there an expression for $Pr(x_1 = x_2)$?

$Pr(x_1 = x_2)$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- If $x_1 = x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{5}{8}$.
- We know $Pr(x_1 = x_2)$ is the same probability as a product with one less transposition.

- If $x_1 \neq x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{3}{8}$.
- This will happen with $Pr(y_1 \neq y_2) = 1 - Pr(x_1 = x_2)$.

- Combining these yield the following probability formula:

$$maxPr(a_1 x_1 a_n = a_n x_2 a_1) = \frac{5}{8} \cdot Pr(x_1 = x_2) + \frac{3}{8} \cdot (1 - Pr(x_1 = x_2))$$

- Is there an expression for $Pr(x_1 = x_2)$?

$Pr(x_1 = x_2)$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- If $x_1 = x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{5}{8}$.
- We know $Pr(x_1 = x_2)$ is the same probability as a product with one less transposition.

- If $x_1 \neq x_2$, $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{3}{8}$.
- This will happen with $Pr(y_1 \neq y_2) = 1 - Pr(x_1 = x_2)$.

- Combining these yield the following probability formula:

$$maxPr(a_1 x_1 a_n = a_n x_2 a_1) = \frac{5}{8} \cdot Pr(x_1 = x_2) + \frac{3}{8} \cdot (1 - Pr(x_1 = x_2))$$

- Is there an expression for $Pr(x_1 = x_2)$?

$Pr(x_1 = x_2)$

Finding maxPr($a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$)

- It seems like something bigger is driving the probability values.
  $ab = ba$
  $abc = cba$
  $abcd = dcba$
  $abcde = edcba$
- What about permutations of the product elements that aren't reversed?
  For example, what is the probability that $abc = bca$?
- Can we find maximum probabilities for these products?

Finding maxPr($a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$)

- It seems like something bigger is driving the probability values.
  $ab = ba$
  $abc = cba$
  $abcd = dcba$
  $abcde = edcba$
- What about permutations of the product elements that aren't reversed?
  For example, what is the probability that $abc = bca$?
- Can we find maximum probabilities for these products?

Finding maxPr($a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1$)

- It seems like something bigger is driving the probability values.
  $ab = ba$
  $abc = cba$
  $abcd = dcba$
  $abcde = edcba$
- What about permutations of the product elements that aren't reversed?
  For example, what is the probability that $abc = bca$?
- Can we find maximum probabilities for these products?

Finding maxPr$(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- It seems like something bigger is driving the probability values.
  $ab = ba$
  $abc = cba$
  $abcd = dcba$
  $abcde = edcba$
- What about permutations of the product elements that aren't reversed?
  For example, what is the probability that $abc = bca$?
- Can we find maximum probabilities for these products?

Rewritable Commutativity

- What about permutations of the product elements that aren't reversed?
- Can we find maximum probabilities for these products?
- YES!! It turns out we can!!

Products	maxPr(comm)
$abcd = cdab$ and $abcde = deabc$	$\frac{5}{8}$
$abcd = cadb$ and $abcdef = aebfdc$	$\frac{17}{32}$
$abcdef = fedcba$ and $abcdef = cfadbe$	$\frac{65}{128}$

Rewritable Commutativity

- Here's the chart again, with a column added showing the number of transpositions.

Products	maxPr(comm)	Transpositions
$abcd = cdab$ and $abcde = deabc$	$\frac{5}{8}$	1
$abcd = cadb$ and $abcdef = aebfdc$	$\frac{17}{32}$	2
$abcdef = fedcba$ and $abcdef = cfadbe$	$\frac{65}{128}$	3

- Wait a minute, $abcdef = aebfdc$ consists of two transpositions? How do you figure that?

Rewritable Commutativity

- What's going on here?
- Let's look at $abc = bca$
- Let $bc = x$. Then $abc = bca$ simplifies to $ax = xa$. Which we can show has $Pr = \frac{5}{8}$.
- Why does this work? Answer: Associativity!!
- What about more complex examples?

Rewritable Commutativity

- For example, what about $abcdef = aebfdc$? How many transpositions are there?
- The first thing to notice is that a is fixed, and can be eliminated using a^{-1}, so that we have $bcdef = ebfdc$.
- Still doesn't look too familiar, but suppose we transpose f and c. Then $eb\mathbf{f}d\mathbf{c}$ becomes $eb\mathbf{c}d\mathbf{f}$, which looks a bit more familiar.
- We still need to switch bcd with e
- Let's use a *block transposition* to exchange bcd and e. But wait, what is a 'block transposition'?

Rewritable Commutativity

Definition

A *block transposition* is a permutation which preserves the order of a string of elements that is transposed with another string of elements, whose order is also preserved.

- For example, the *block transposition* ([2,3],[5,6,7]) of the product $abcdefgh$ becomes $aefgdbch$.
- As a note, all transpositions can be considered *block transpositions*, just with both strings of elements containing one element.

Rewritable Commutativity

$$abcdef^{([2,3,4],[5])} \Rightarrow aebcdf^{([4],[6])} \Rightarrow aebfdc$$

- So it turns out that $abcdef = aebfdc$ has two transpositions.
- One block transposition switches bcd and e, making the product $aebcdf$
- The second is a regular transposition switching c and f, to make the final product, $aebfdc$.
- Those two transpositions mean that $maxPr = \frac{17}{32}$.

Rewritable Commutativity

$$abcdef^{([2,3,4],[5])} \Rightarrow aebcdf^{([4],[6])} \Rightarrow aebfdc$$

- So it turns out that $abcdef = aebfdc$ has two transpositions.
- One block transposition switches bcd and e, making the product $aebcdf$
- The second is a regular transposition switching c and f, to make the final product, $aebfdc$.
- Those two transpositions mean that $maxPr = \frac{17}{32}$.

Rewritable Commutativity

$$abcdef^{([2,3,4],[5])} \Rightarrow aebcdf^{([4],[6])} \Rightarrow aebfdc$$

- So it turns out that $abcdef = aebfdc$ has two transpositions.
- One block transposition switches bcd and e, making the product $aebcdf$
- The second is a regular transposition switching c and f, to make the final product, $aebfdc$.
- Those two transpositions mean that $maxPr = \frac{17}{32}$.

Rewritable Commutativity

$$abcdef^{([2,3,4],[5])} \Rightarrow aebcdf^{([4],[6])} \Rightarrow aebfdc$$

- So it turns out that $abcdef = aebfdc$ has two transpositions.
- One block transposition switches bcd and e, making the product $aebcdf$
- The second is a regular transposition switching c and f, to make the final product, $aebfdc$.
- Those two transpositions mean that $maxPr = \frac{17}{32}$.

Finding $maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1)$

- We can generalize our table to the following, basing the probability on the number of block transpositions in the product.

Transpositions	maxPr(comm)
1	$\frac{5}{8}$
2	$\frac{17}{32}$
3	$\frac{65}{128}$

- Which leads to the formula:

$$maxPr(a_1\cdots a_n = (a_1\cdots a_n)^\sigma) = \frac{2^{2k}+1}{2^{2k+1}}$$

where k is the number of *block transpositions* caused by σ.

- Substituting this formula in for $Pr(x_1 = x_2)$ and manipulating yields the formula:

$$maxPr(a_1a_2\cdots a_n = a_n\cdots a_2a_1) = \frac{1}{2} + \frac{1}{2^{2k+1}} \quad \text{where } k = \lfloor \tfrac{n}{2} \rfloor$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We can generalize our table to the following, basing the probability on the number of block transpositions in the product.

Transpositions	maxPr(comm)
1	$\frac{5}{8}$
2	$\frac{17}{32}$
3	$\frac{65}{128}$

- Which leads to the formula:

$$maxPr(a_1 \cdots a_n = (a_1 \cdots a_n)^\sigma) = \frac{2^{2k}+1}{2^{2k+1}}$$

where k is the number of *block transpositions* caused by σ.

- Substituting this formula in for $Pr(x_1 = x_2)$ and manipulating yields the formula:

$$maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{1}{2} + \frac{1}{2^{2k+1}} \quad \text{where } k = \lfloor \frac{n}{2} \rfloor$$

Finding $maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1)$

- We can generalize our table to the following, basing the probability on the number of block transpositions in the product.

Transpositions	maxPr(comm)
1	$\frac{5}{8}$
2	$\frac{17}{32}$
3	$\frac{65}{128}$

- Which leads to the formula:

$$maxPr(a_1 \cdots a_n = (a_1 \cdots a_n)^\sigma) = \frac{2^{2k}+1}{2^{2k+1}}$$

where k is the number of *block transpositions* caused by σ.

- Substituting this formula in for $Pr(x_1 = x_2)$ and manipulating yields the formula:

$$maxPr(a_1 a_2 \cdots a_n = a_n \cdots a_2 a_1) = \frac{1}{2} + \frac{1}{2^{2k+1}} \quad \text{where } k = \lfloor \tfrac{n}{2} \rfloor$$

Resources and Acknowledgements

- Dr. Tom Langley
  Dr. Langley came up with the basic context of the problem, during Abstract Algebra.
- The CLU math department especially Dr. Fogel, my fellow undergrads and particularly Alex Sherbetjian.

- Gallian, Joseph A. *Contemporary Abstract Algebra*, 6th Edition. Houghton Mifflin, 2006.
  The book is the textbook for Abstract Algebra, and has often been consulted for the necessary definitions.
- Sherman, GJ. *Trying to do Group Theory with Undergraduates and Computers*. J. Symbolic Computation (1997) 23, 577-587.
- GAP computational software
  Computations determining the maximum probability of product strings were found using GAP.