Using Graph Theory to Investigate the Size of a Random Product or Quotient Set

June Duvivier[1], Xiaoyao Huang[2], Ava Kennon[3], Say-Yeon Kwon[4], Steven J. Miller[5], Arman Rysmakhanov[5], Pramana Saldin[6], Ren Watson[7]

[1]Reed College, [2]University of Michigan, [3]Amherst College, [4]Princeton University, [5]Williams College, [6]University of Wisconsin, [7]University of Texas at Austin

Product and Quotient Sets

Let G be a finitely presented multiplicative group equipped with a word metric. Let $A = \{a_1, \ldots, a_n\} \subseteq G$ and let $A^{-1} := \{a_1^{-1}, \ldots, a_n^{-1}\}$. The ***product set*** and the ***right*** and ***left difference sets*** of A are given, respectively, by

$$AA := \{a_i \cdot a_j : a_i, a_j \in A\},$$
$$AA^{-1} := \{a_i \cdot a_j^{-1} : a_i, a_j \in A\},$$
$$A^{-1}A := \{a_i^{-1} \cdot a_j : a_i, a_j \in A\}.$$

Following Lazarev-Miller-O'Bryant [1], we use graph theory as a framework to compute the probability that AA or AA^{-1} contain a word of a specified length, where A is random.

Condition Graphs

Let $R \geq 0$ and B_R be the set of words in G of length $\leq R$. **What can we say about the size of a uniform random subset A of B_R?**

Definition

The ***condition graph*** $C(w_1, \ldots, w_k \notin AA^{-1})$ is a graph with vertex set G and edges (u, v) whenever $uv^{-1} = w_i$ or $u^{-1}v = w_i$ for some $i \in \{1, \ldots, k\}$.

Similarly, the condition graph $C(w_1, \ldots, w_k \notin AA)$ is a graph with vertex set G and edges (u, v) whenever $uv = w_i$ or $vu = w_i$ for some $i \in \{1, \ldots, k\}$.

The condition graph $C(w_1, \ldots, w_k \notin S)$ represents all the ways that the words $w_1, \ldots, w_k$ could appear as an element of S through a specified random process. In order to consider questions of probability, we restrict our attention to the subgraphs $C_R(w_1, \ldots, w_k \notin S)$ induced by B_R, the set of all words in G of length $\leq R$.

The connected components of the condition graph $C(w \notin AA^{-1})$ are paths and cycles.

Lemma. Structure of $C(w \notin AA^{-1})$.

Let X be a connected component of of $C(w \notin AA^{-1})$. Then, X is isomorphic to one of the following.

(1) A cycle;
(2) A path of infinite length;
(3) A path of length 2;
(4) A singleton.

Case 3 occurs only when w is a square. Case 4 only occurs when $w = e$, in which case every connected component is a singleton.

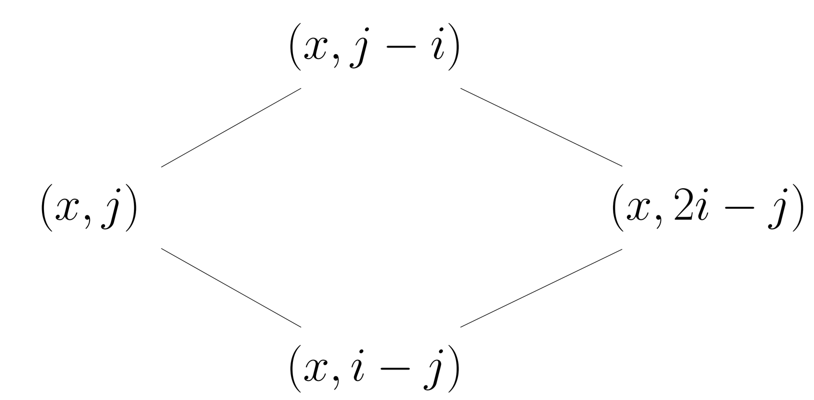
Counting the numbers of path and cycle connected components allows us to determine the probability that $w \notin AA^{-1}$. Let $p(k)$ be the number of length k path components in $C_R(w \notin S)$ and $c(k)$ be the number of length k cycle components in $C_R(w \notin S)$. Then, we have the following formula in terms of the Fibonacci numbers $F_1 = 1$, $F_2 = 2$, and $F_k = F_{k-1} + F_{k-2}$.

$$\mathbb{P}(w \notin AA^{-1}) = \prod_{k=1}^{\infty} \left(\frac{F_{k+1}}{2^k}\right)^{p(k)} \prod_{k=1}^{\infty} \left(\frac{F_{k-2} + F_k}{2^k}\right)^{c(k)}.$$

Condition Graphs for $\mathbb{Z}_2 * \mathbb{Z}_2$

Words in $\mathbb{Z}_2 * \mathbb{Z}_2$ are alternating strings of x, y. Any word can be encoded as a pair (c, i) where c is the starting character (either x or y) and i is the length of the string. In $\mathbb{Z}_2 * \mathbb{Z}_2$, the condition graphs $C_R(w \notin AA)$ have paths and cycles.

Example. If $w = (x, i)$ and $j \geq 1$ is odd, we have the cycle



Theorem. $C_R(w \notin AA)$ in $\mathbb{Z}_2 * \mathbb{Z}_2$

Let $w \in \mathbb{Z}_2 * \mathbb{Z}_2$. Then for AA,

(1) $C_R(e)$ consists of $\begin{cases} 2\lceil \frac{R}{2} \rceil + 1 \text{ self-loops,} \\ \lfloor \frac{R}{2} \rfloor \text{ paths of length 1.} \end{cases}$

(2) **if w is of even length $i \geq 2$,** write $R = k(\frac{i}{2}) + j$ for $j, k \in \mathbb{Z}_{\geq 0}$ and $j < \frac{i}{2}$. Then,

(i) **if $4 \mid i$,** $C_R(w)$ consists of $\begin{cases} 2\lceil \frac{j}{2} \rceil \text{ paths of length } k \text{ if } k \geq 1, \\ \frac{i}{2} - 2\lceil \frac{j}{2} \rceil \text{ paths of length } k-1 \text{ if } k \geq 2, \\ \lfloor \frac{2R-i-2}{4} \rfloor \text{ paths of length 1 if } R \geq \frac{i}{2}, \\ 1 \text{ self-loop if } R \geq \frac{i}{2}. \end{cases}$

(ii) **if $4 \nmid i$,** $C_R(w)$ consists of
$\begin{cases} j+1 \text{ (resp. } j) \text{ paths of length } k \text{ if } k \geq 1, R \text{ odd (resp. even),} \\ \frac{i}{2} - j - 1 \text{ (r. } \frac{i}{2} - j) \text{ paths of length } k-1 \text{ if } k \geq 2, R \text{ odd (r. even),} \\ \lfloor \frac{2R-i}{4} \rfloor \text{ paths of length 1 if } R \geq \frac{i}{2}. \end{cases}$

(3) **if w is of odd length i,** then $C_R(w)$ consists of
$\begin{cases} \lfloor \frac{R-i}{2} \rfloor \text{ 4-cycles if } R \geq i, \\ R - \lfloor \frac{i}{2} \rfloor \text{ paths of length 2 if } \lfloor \frac{i}{2} \rfloor < R < i, \\ \lfloor \frac{R}{2} \rfloor - \lfloor \frac{R-i}{2} \rfloor \text{ paths of length 2 if } R \geq i, \\ 1 \text{ path of length 1 if } R \geq i. \end{cases}$

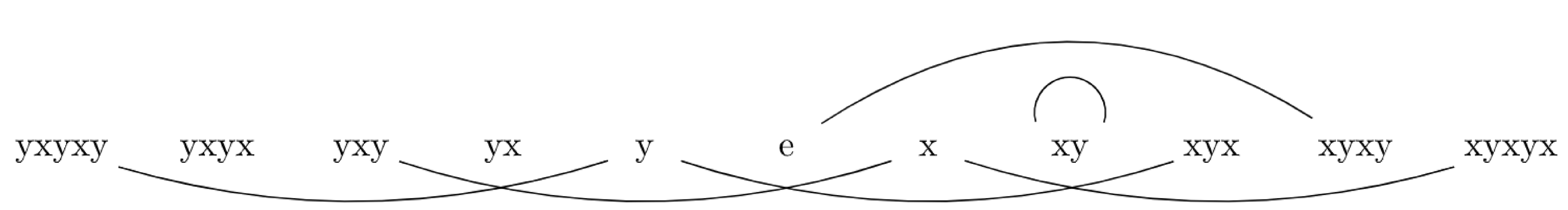


Figure 1: $C_5(xyxy)$ for AA.

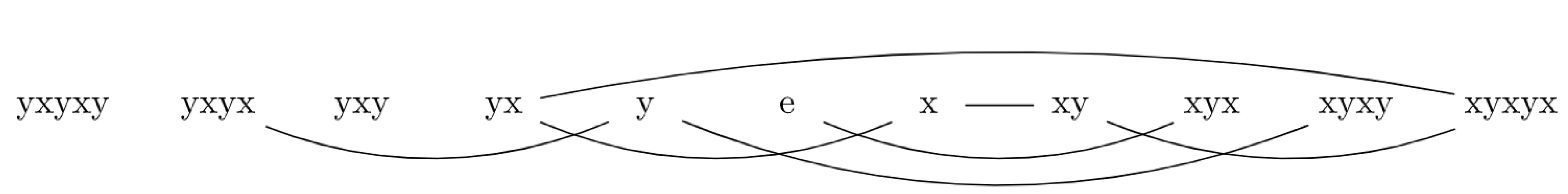


Figure 2: $C_5(xyx)$ for AA.

$\mathbb{Z}_2 * \mathbb{Z}_2$ Continued

Theorem. $C_R(w \notin AA^{-1})$ in $\mathbb{Z}_2 * \mathbb{Z}_2$)

Let $w \in \mathbb{Z}_2 * \mathbb{Z}_2$. Then,

(1) $C_R(e \notin AA^{-1})$ consists of $2R + 1$ self-loops.

(2) **if w is of even length $i \geq 2$,** write $R = k(\frac{i}{2}) + j$ for $j, k \in \mathbb{Z}_{\geq 0}$ and $j < \frac{i}{2}$. Then, $C_R(w \notin AA^{-1})$ consists of
$\begin{cases} 2j + 1 \text{ paths of length } k \text{ if } k \geq 1, \\ i - 2j - 1 \text{ paths of length } k - 1 \text{ if } k \geq 2. \end{cases}$

(3) **if w is of odd length i,** then $C_R(w \notin AA^{-1})$ consists of $R - \lfloor \frac{i}{2} \rfloor$ paths of length 1 if $R \geq \frac{i}{2}$.

Using the Lemma, we can find $\mathbb{P}(w \notin AA^{-1})$ in each of these cases where $A \subseteq B_R$ and R is sufficiently large.

Future Work

We hope to extend the condition graphs framework to

(1) Condition graphs $C(w_1, \ldots, w_k \notin S)$ on $\mathbb{Z}_2 * \mathbb{Z}_2$ involving multiple words;
(2) The free group F_2 (partial progress);
(3) Random subsets A where each element is included indpendently with probability p (not just $p = 1/2$).

On the free group on 2-generators F_2, we have made progress when all elements of A are of uniform length. In this case,

$$\mathbb{P}(w \notin AA^{-1}) = \begin{cases} 0 & |w| \text{ odd} \\ (\frac{3}{4})^{3^{R-|w|/2}} & |w| \text{ even and middle characters the same} \\ (\frac{3}{4})^{2*3^{R-|w|/2-1}} & |w| \text{ even and middle characters different.} \end{cases}$$

This work also suggests ways to compute the expected sizes $\mathbb{E}|AA|$ and $\mathbb{E}|AA^{-1}|$ as well as the variances $\text{Var}|AA|$ and $\text{Var}|AA^{-1}|$.

References

[1] Oleg Lazarev, Steven J. Miller, and Kevin O'Bryant.
Distribution of missing sums in sumsets.
Exp. Math., 22(2):132–156, 2013.

[2] G Martin and K O'Bryant.
Many sets have more sums than differences, Additive combinatorics, 287–305.
In *CRM Proc. Lecture Notes*, volume 43.

Acknowledgements

We are grateful to Professor Steven J. Miller for his mentorship. This research was supported by the National Science Foundation, under NSF Grant DMS2241623, Amherst College, Princeton University, the University of Wisconsin, the University of Michigan, and the Finnerty Fund.