On the Multiplicative Structure of Cyclic Semirings

Jiya Dani, Bryan Li, and Arav Paladiya

(Research Mentors: Felix Gotti, Marly Gotti, Joseph Vulakh)

CrowdMath Internship

SWIM 2025
August 12, 2025

Outline

- Background
- Group of Units
- Factorization Properties

General Notations

Some General Notation

- $\mathbb{N}$ denotes the set of positive integers.
- $\mathbb{N}_0$ denotes the set of non-negative integers.
- $\mathbb{P}$ denotes the set of (positive) primes.
- $\mathbb{A}$ denotes the set of algebraic complex numbers.
- $\mathbb{C}$ denotes the set of complex numbers.

Commutative Cancellative Monoids

Definition. A monoid is a pair $(M, +)$, where M is a set and $+$ is an associative binary operation on M such that there exists an element $0 \in M$ with $0 + b = b + 0 = b$ for all $b \in M$.

Note. Throughout this presentation, we tacitly assume that every monoid M is

- commutative: $b + c = c + b$ for all $b, c \in M$ and
- cancellative: $a, b, c \in M$, if $a + c = b + c$, then $a = b$.

We check that the following are indeed monoids, because they satisfy closure, have an identity, and are also commutative and cancellative.

Examples

- $(\mathbb{N}_0, +)$: The nonnegative integers.
- $(\{0\} \cup \mathbb{Q}_{\geq 1}, +)$: The rationals that are at least 1, and 0.
- $(\mathbb{Q}_{\geq 1}, \cdot)$: Rationals that are at least 1 (under multiplication).

Submonoids

We say that N is a submonoid of M if $N \subseteq M$ and N itself is a monoid under the same operation (i.e., N is closed, has an identity, and satisfies associativity, commutativity, and cancellativity).

Examples.

- A numerical monoid is defined as a submonoid of $(\mathbb{N}_0, +)$ with finite complement.
- A Puiseux monoid is defined as a submonoid of $(\mathbb{Q}_{\geq 0}, +)$.
- Every numerical monoid is also a Puiseux monoid.

Generating Set and Finitely Generated Monoids

An additive monoid M is generated by $S \subseteq M$, or $M = \langle S \rangle$, if

$$M = \{c_1 s_1 + \cdots + c_n s_n : s_i \in S, c_i \in \mathbb{N}\}.$$

$\langle S \rangle$ is the set that consists of all finite linear combinations of elements in S.

If $M = \langle S \rangle$, we can say that S is a generating set of M.

We say that M is finitely generated if we can find a finite set S such that $M = \langle S \rangle$.

Examples of Generating Sets

Examples.

- Numerical monoids, such as $\langle 3, 5\rangle := \{0, 3, 5, 6\} \cup \mathbb{N}_{\geq 8}$, are all finitely generated.
- The (multiplicative) Hilbert monoid $H := 4\mathbb{N}_0 + 1$ is commutative and cancellative, but not finitely generated.
- The Puiseux monoid $M := \langle \frac{1}{p} : p \in \mathbb{P}\rangle$ is a submonoid of $G := \langle \frac{1}{2^i p_i} : i \in \mathbb{N}\rangle$, where p_i is the ith odd prime.

Units, Atoms, and Atomic Monoids

Definitions. Let M be a monoid.

- An element $u \in M$ is a unit if $u + v = 0$ for some $v \in M$ (in additive notation).
- A non-unit $a \in M$ is an atom (or irreducible element) if a cannot be written as a sum of two non-units.
- The monoid M is atomic if each non-unit can be written as a finite sum of atoms (allowing repetitions).

Examples.

- In $(\mathbb{N}, \cdot)$, the only unit is 1, and we can check that the atoms are the primes.
- Every element except 0 in the monoid $(\mathbb{Q}, \cdot)$ is a unit.

Groups

A group has all the properties of a monoid, with the additional requirement that all elements must have inverses (i.e. every element is a unit).

If a group is commutative, we say that it is an abelian group.

Examples.

- $(\mathbb{Z}, +)$ is a group; for every element $n \in \mathbb{Z}$, we have that $-n \in \mathbb{Z}$ as well.
- $(\mathbb{Q}_{>0}, \cdot)$ is a group. Every positive rational has a multiplicative inverse that is also a positive rational!
- $(\mathbb{Q}_{\geq 0}, \cdot)$ and $(\mathbb{Q}_{\geq 1}, \cdot)$ are monoids, but not groups. Why?

Rings and Integral Domains

Definition. A ring is a triple $(R, +, \cdot)$ such that

- $(R, +, 0)$ is an abelian group,
- $(R, \cdot, 1)$ is a commutative monoid, and
- $a(b + c) = ab + ac$ for all $a, b, c \in R$ (distributive law).

Definition. An integral domain is a ring R with the property that for any $a, b \in R$, we have that $a \cdot b = 0$ implies $a = 0$ or $b = 0$.

Examples.

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$: integral domains.
- $\mathbb{Z}_4$ (integers modulo 4): ring but not an integral domain.

Semirings and Semidomains

Definition. A semiring (resp. semidomain) is a ring (resp. integral domain) without additive inverses.

Examples.

- $\mathbb{N}_0$: semiring, not a ring.
- $\mathbb{Q}_{\geq 0}$: semiring, not a ring.
- $\mathbb{N}_0[x]$: semidomain of polynomials.

Minimal Polynomial and Algebraic Conjugates

Recall that an algebraic number is a root of a polynomial in $\mathbb{Q}[x]$, the ring consisting of all polynomials with rational coefficients.

For $\alpha \in \mathbb{A}$, the minimal polynomial $m(x) \in \mathbb{Q}[x]$ of α is the unique monic polynomial with minimum degree such that $m(\alpha) = 0$.

The algebraic conjugates of α are all the roots of $m(x)$.

Examples.

- The minimal polynomial of $\sqrt[3]{3}$ is $x^3 - 3$.
- The minimal polynomial of $\frac{-3+\sqrt{3}i}{2}$ is $x^2 + 3x + 3$, and its algebraic conjugates are itself, and its complex conjugate, $\frac{-3-\sqrt{3}i}{2}$.

Algebraic Numbers and Integers

An algebraic integer is an algebraic number whose minimal polynomial is in $\mathbb{Z}[x]$.

For an algebraic integer α, we define the number field $K = \mathbb{Q}(\alpha)$ as the field containing the elements of the form $\sum_{i=0}^{d-1} q_i \alpha^i$, where each q_i is a rational and d is the degree of the minimal polynomial of α.

The ring of integers of a number field K, denoted as $\mathcal{O}_K$, is the ring of all algebraic integers in K.

Example of an Algebraic Number Field

Example: The algebraic number i is an algebraic integer as its minimal polynomial is $x^2 + 1 \in \mathbb{Z}[x]$. The number field $K = \mathbb{Q}(i)$ contains all elements of the form $a + bi$, which $a, b \in \mathbb{Q}$. We will show that $\mathcal{O}_K = \mathbb{Z}[i]$

- Any $\beta = a + bi$ is the root of $m(x) = x^2 - 2ax + (a^2 + b^2)$.
- If $a, b \in \mathbb{Z}$, then $m(x) \in \mathbb{Z}[x]$ and thus β is an algebraic integer.
- If a is not an integer, then the only way for the $2ax$ term of $m(x)$ to be an integer is if $a = \frac{k}{2}$ for some odd integer k.
- This means that $k^2 \equiv 1 \pmod 4$. The only way for $a^2 + b^2 = \frac{k^2}{4} + b^2$ to be an integer is if $k^2 + 4b^2$ is an integer.
- However, this implies that $4b^2 \equiv 3 \pmod 4$, which is impossible when b is rational.
- Thus $\beta \in \mathcal{O}_K$ if and only if $\beta \in \mathbb{Z}[i]$, so we have $\mathcal{O}_K = \mathbb{Z}[i]$ as desired.

Simple Extensions of $\mathbb{N}_0$

Definition. For $\alpha \in \mathbb{C}$, we define

$$\mathbb{N}_0[\alpha] := \{f(\alpha) : f(x) \in \mathbb{N}_0[x]\}$$

This is a prototypical example of a cyclic semidomain.

Theorem. For $\alpha \in \mathbb{A}$, the semidomain $\mathbb{N}_0[\alpha]$ is an integral domain if and only if α has no positive conjugates.

In this case, $\mathbb{N}_0[\alpha] = \mathbb{Z}[\alpha]$.

This theorem plays a central role in our analysis.

Group of Units

The set of all units of any monoid turns out to be a group!

The set of units...

- is closed under the operation of the monoid. (If u has inverse u^{-1} and v has inverse v^{-1}, then $u \cdot v$ has inverse $v^{-1} \cdot u^{-1}$.)
- contains the identity element.
- satisfies associativity, cancellativity, and commutativity, as a result of being a subset of the monoid which satisfies all these properties.

For a multiplicative monoid M, we denote its group of units as $M^\times$.

Example.

- Consider the monoid $\mathbb{N}_0[\frac{1}{2}] = \langle \frac{1}{2^k} : k \in \mathbb{N}_0 \rangle$. Then, $\mathbb{N}_0[\frac{1}{2}]^\times = \{2^k : k \in \mathbb{Z}\}$. This is because $\frac{2^k}{n} \in \mathbb{N}_0[\frac{1}{2}]$ only if n is a power of 2.

Group and Monoid Isomorphisms

For groups $(G, *)$ and $(H, \cdot)$, we say that G is isomorphic to H if there exists a bijective function $f : G \to H$ such that $f(a * b) = f(a) \cdot f(b)$ for all $a, b \in G$. If G and H are isomorphic, we can write $G \cong H$.

More intuitively, this just means that G and H have the same structure.

This definition also applies to monoids $(G, *)$ and $(H, \cdot)$.

Examples.

- $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$ because $f(a + b) = f(a)f(b)$ for $f(x) = e^x$ for all $a, b \in \mathbb{R}$.
- $\mathbb{Z}_4$ is isomorphic to $(\{1, i, -1, -i\}, \cdot)$. Consider the function $f(x) = e^{\frac{2\pi i x}{4}}$ that maps 0 to 1, 1 to i, 2 to -1, and 3 to $-i$.

Finite Cyclic Groups and Roots of Unity

We call a group G cyclic if there exists an element $a \in G$ such that $G = \langle a \rangle = \{\ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots\}$.

If this group has finitely many elements (i.e. $a^j = a^k$ for some $j \neq k$, $j, k \in \mathbb{Z}$), then we call it a finite cyclic group of size n, where n is the number of elements the group contains. Such a group can be denoted by C_n.

Note that every finite cyclic group of size n is isomorphic to $\mathbb{Z}_n$.

An nth root of unity is one of the n solutions to the equation $x^n = 1$. The set of solutions is $\left\{e^{\frac{2\pi ik}{n}} : 0 \leq k \leq n-1\right\}$. This is in fact a finite cyclic group of size n under multiplication!

Example.

- The fourth roots of unity are the solutions to $x^4 = 1$, which are 1, -1, i, and $-i$.

Dirichlet's Unit Theorem

Dirichlet's Unit Theorem. Let α be an algebraic integer with minimal polynomial $m(x)$. Then:

$$\mathbb{Z}[\alpha]^\times \cong \mathbb{Z}^{r_1+r_2-1} \times \mu$$

where r_1 is the number of real roots, r_2 is the number of complex conjugate pairs, and μ is the finite cyclic group of roots of unity in $\mathbb{Z}[\alpha]$.

Historical Note: Established by Dirichlet (1846), this landmark result reveals that the group of units in a number ring is finitely generated.

Group of Units of Cyclic Semidomains

Proposition. [Dani-Li-Paladiya, 2025] Let α be algebraic such that $\mathbb{N}_0[\alpha]$ is not an integral domain. If $\mathbb{N}_0[\alpha]^\times$ is nontrivial, then $\alpha^n \in \mathbb{N}_0[\alpha]^\times$ for all $n \in \mathbb{N}_0$, which is equivalent to the additive monoid being antimatter.

Theorem.[Dani-Li-Paladiya, 2025] Let β be an algebraic number.

- If $\beta > 0$, then $\mathbb{N}_0[\beta]^\times \cong \mathbb{Z}^n$.
- Otherwise, $\mathbb{N}_0[\beta]^\times \cong C_k \times \mathbb{Z}^n$.

This generalizes Dirichlet's theorem to certain semiring settings.

First Example of the Group of Units

Example. The group of units of $\mathbb{N}_0\left[\frac{1}{6}\right]$ is isomorphic to $\mathbb{Z}^2$.

- First, $\frac{1}{6^k} \in \mathbb{N}_0[\frac{1}{6}]$ for $k \in \mathbb{N}_0$, and we can multiply this by $2^m 3^n$ for $m, n \in \mathbb{N}_0$ to get $2^{m-k}3^{n-k}$. Since $(m-k, n-k)$ can cover all of $\mathbb{Z}^2$, we can obtain all $2^a 3^b \in \mathbb{N}_0[\frac{1}{6}]$ for $a, b \in \mathbb{Z}$.
- Since $2^a 3^b, 2^{-a}3^{-b} \in \mathbb{N}_0\left[\frac{1}{6}\right]$ for all $a, b \in \mathbb{Z}$, this implies $2^a 3^b$ are units for all integers a, b.
- It is then clear that any element not of this form cannot be a unit; its inverse would have a prime number (not equal to 2 or 3) as a divisor the denominator.
- Thus, we have $\mathbb{N}_0\left[\frac{1}{6}\right]^\times = \{2^a 3^b : a, b \in \mathbb{Z}\} \cong \mathbb{Z}^2$.

Second Example of the Group of Units (part 1)

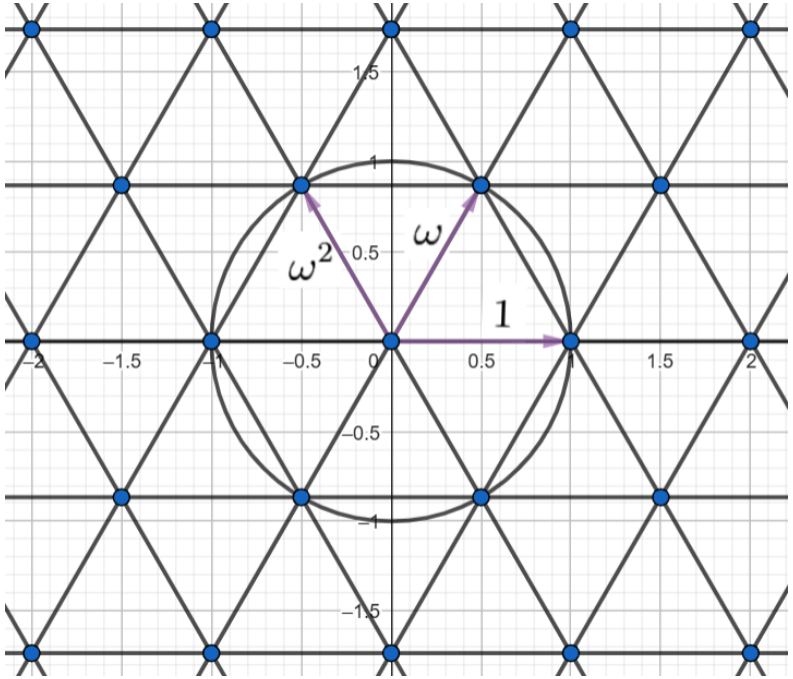
Example. Let α be a root of $x^2 + 3x + 3$. Let us show that $\mathbb{N}_0[\alpha]^\times$ is generated by $\alpha + 2$.

This group is finite and contains precisely the sixth roots of unity. Thus, it is isomorphic to C_6.

- Suppose $\alpha = \frac{-3+\sqrt{3}i}{2}$. Notice that $\alpha + 2 = e^{\frac{2\pi i}{6}}$ and $\alpha + 1 = e^{\frac{2\pi i}{3}}$.
- Letting $\omega = \alpha + 2$, we have $\omega^2 = \alpha + 1$.
- This gives $\alpha = \alpha + (\alpha^2 + 3\alpha + 3) = (\alpha + 3)(\alpha + 1) = (\omega + 1) \cdot \omega^2$
- Since α has no positive conjugates, we can work in $\mathbb{Z}[\alpha]$.
- Any element of $\mathbb{N}_0[\alpha]$ can be written as $f(\alpha) = \sum c_i \alpha^i$, $c_i \in \mathbb{Z}$.

Second Example of the Group of Units (part 2)

- Because we know $\omega^3 = -1$, we can make the substitution $\alpha = (\omega + 1) \cdot \omega^2$ into $f(\alpha)$, and simplify until we get $f(\alpha) = a + b\omega + c\omega^2$ for some $a, b, c \in \mathbb{Z}$.
- Any $a + b\omega + c\omega^2$ must lie on a vertex of this equilateral triangle tiling of the complex plane. From here, we obtain that the units must be precisely those that lie on the unit circle.



The Unique Factorization Property

Definition. A monoid M (resp. integral domain M) is a UFM (resp. UFD) if every element of M has only one factorization up to multiplication by units and ordering of its atoms.

- $\mathbb{Z}$ is a UFD.
- $\mathbb{Z}[x]$ is a UFD, but $\mathbb{N}_0[x]$ is not a UFS.
- Indeed, we can observe that $(x^3+1)(x^2+x+1)$ and $(x^4+x^2+1)(x+1)$ both equal $x^5+x^4+x^3+x^2+x^1+1$. It can be shown that both elements of each factorization are atoms, and so these are two distinct factorizations of the same element.

More Examples of UFDs

- $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ is a UFD.
- However, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. In fact, $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. We can show that these elements are irreducible and not associates of each other, so they are distinct factorizations.

It is actually not known whether there are infinitely many $d \in \mathbb{N}$ so that $\mathbb{Z}[\sqrt{d}]$ is a UFD. When d is negative, the ring $\mathbb{Z}[\sqrt{d}]$ is a UFD precisely when d is one of $-1, -2, -3, -7, -11, -19, -43, -67, -163$.

UFD Proposition

Proposition. [Dani-Li-Paladiya, 2025] Let α be an algebraic integer whose minimal polynomial has no positive roots and let $n \in \mathbb{N}$. Then, if $\mathbb{N}_0[\alpha]$ is a UFD, we also have that $\mathbb{N}_0[\frac{\alpha}{n}]$ is a UFD.

Insight. The UFD property for algebraic integers always descends to scaled extensions.

Example. Recall that $\mathbb{Z}[i]$ is a UFD. As the conjugates of i are $\pm i \notin \mathbb{R}_{>0}$, we have that $\mathbb{Z}[i] = \mathbb{N}_0[i]$. It follows from the Proposition that $\mathbb{N}_0[\frac{i}{n}]$ is a UFD for any $n \in \mathbb{N}$.

Finite Factorization

Definition. A monoid is an FFM if it is atomic and each nonunit has only finitely many factorizations into irreducibles, up to order and multiplication by units.

Similarly, semidomains and integral domains satisfying the finite factorization property are called FFS and FFD, respectively.

Note that the unique factorization property is stronger than finite factorization.

- The ring of integers $\mathbb{Z}$ is an FFD as it is a UFD
- The monoid $\langle 2, 3 \rangle$ under addition is an FFM.

An Example Not Satisfying FF

Here is an example of a monoid that is atomic but not an FFM.

Example. The monoid $M = \langle \frac{1}{p} : p \in \mathbb{P} \rangle$ is **not** an FFM.

- First observe that each $\frac{1}{p}$ for $p \in \mathbb{P}$ is irreducible.
- If we have $\frac{a}{b} + \frac{c}{d} = \frac{1}{p}$, then $\frac{1}{p} = \frac{ad+bc}{bd}$. Then either $p \mid b$ or $p \mid d$, but this forces one of a or c to be 0.
- The element 1 has infinitely many factorizations: $1 = \frac{1}{p} + \frac{1}{p} + \cdots + \frac{1}{p}$ for all $p \in \mathbb{P}$.

Finite Factorization Monoids

Theorem. [Deng-Zeng, 2025] $\mathbb{N}_0[q]$ is an FFM if and only if:

1. $q \in \mathbb{N}^{\pm 1}$;
2. the denominator of $q = \frac{a}{b} \in (0,1) \cap \mathbb{Q}$, with $\gcd(a,b) = 1$, is a power of a prime;
3. $q \geq 1$.

Remark: $q > 1$ turns $\mathbb{N}_0[q]$ into an FFS because $\ln \mathbb{N}_0[q]^*$ is a positive monoid generated by an increasing sequence (which is known to be an FFM by Gotti [Theorem 5.6] in "Increasing positive monoids of an ordered fields are FF").

Implication. The arithmetic of $\mathbb{N}_0[q]$ is highly sensitive to the nature of q.

A Useful Isomorphism Between Cyclic Semirings

Proposition. Let α have minimal polynomial $m(x)$, and let β be a root of $m(x)$. Then $\mathbb{N}_0[\alpha] \cong \mathbb{N}_0[\beta]$.

- The isomorphism $\varphi : \mathbb{N}_0[\alpha] \to \mathbb{N}_0[\beta]$ is given by $\varphi(f(\alpha)) = f(\beta)$, where $f(\alpha) \in \mathbb{N}_0[\alpha]$ with $f(x) \in \mathbb{N}_0[x]$.
- It can be verified that this map is in fact multiplicative and a bijection, and also that it is well defined.

The Finite Factorization Property (part 1)

Proposition. Let α be an algebraic integer. If α has a real algebraic conjugate β such that $\beta > 1$, then $\mathbb{N}_0[\alpha]$ is an FFS.

- Since β is an algebraic conjugate of α, from the proposition on the previous slide we have that $\mathbb{N}_0[\alpha] \cong \mathbb{N}_0[\beta]$. Hence both semidomains have the same structure and the same factorization properties.
- If $\beta > 1$, then we have that for each element $m \in \mathbb{N}_0[\beta]$, there are finitely many elements less than m (and all elements are at least 1).
- Then, the number of distinct factorizations of m is at most

$$\prod_{e \in \mathbb{N}_0[\beta], 1 < e < m} \lfloor \log_e(m) \rfloor,$$

which is finite. Thus, $\mathbb{N}_0[\beta]$ is an FFS, and so is $\mathbb{N}_0[\alpha]$.

The Finite Factorization Property (part 2)

Proposition. [Dani-Li-Paladiya, 2025] Let α be an algebraic integer whose minimal polynomial has no positive real roots. Then $\mathbb{N}_0[\alpha]$ is an FFD.

Proposition. [Hong et al. 2025 & Dani-Li-Paladiya, 2025] Let α be algebraic and $\mathbb{N}_0[\alpha]^\times = \{1\}$. Then $\mathbb{N}_0[\alpha]$ is an FFD iff for every a, the set

$$S := \{u \in \mathbb{Z}[\alpha]^\times : au, au^{-1} \in \mathbb{N}_0[\alpha]\}$$

is finite.

Remark. This links the finiteness of factorizations to the ambient unit group.

References

- D. D. Anderson, D. F. Anderson, and M. Zafrullah, *Factorizations in integral domains*, J. Pure Appl. Algebra **69** (1990) 1–19.
- D. F. Anderson and F. Gotti, *On the bounded and finite factorization property*.
- S. T. Chapman, F. Gotti, and M. Gotti, *Factorization invariants of Puiseux monoids generated by geometric sequences*, Comm. Algebra **48** (2020) 380–396.
- J. Correa-Morris and F. Gotti, *On the additive structure of algebraic valuations of polynomial semirings*, J. Pure Appl. Algebra **226** (2022) 107104.
- D. R. Curtiss, *Recent extensions of Descartes' rule of signs*, Ann. Math. **19** (1918) 251–278.

References

- A. Dubickas, *On roots of polynomials with positive coefficients*, Manuscripta Math. **123** (2007) 353–356.
- A. Geroldinger and F. Halter-Koch, *Non-unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics Vol. 278, Chapman & Hall/CRC, Boca Raton, 2006.
- F. Gotti: *Increasing positive monoids of ordered fields are FF-monoids*, J. Algebra **518** (2019) 40–56.
- A. Grams, *Atomic domains and ascending chain conditions on principal ideals*, Math. Proc. Cambridge Philos. Soc. **75** (1974) 321–329.
- F. Halter-Koch, *Finiteness theorems for factorizations*, Semigroup Forum **44** (1992) 112–117.

Acknowledgments

- We thank the SWIM organizers for making it possible to present our work through this workshop.
- We thank our mentors Felix Gotti, Marly Gotti, and Joseph Vulakh for their guidance on our research.
- Lastly, we thank the CrowdMath Internship program for providing us the opportunity to do this research project.

End of Presentation

THANK YOU!