

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

LÊ THỊ THU THỦY

VỀ NỬA NHÓM SỐ MERSENNE

LUẬN VĂN THẠC SĨ TOÁN HỌC

Nghệ An - 2022

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

LÊ THỊ THU THỦY

VỀ NỬA NHÓM SỐ MERSENNE

Chuyên ngành: ĐẠI SỐ VÀ LÝ THUYẾT SỐ
Mã số: 846 01 04

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học
PGS. TS. NGUYỄN THỊ HỒNG LOAN

Nghệ An - 2022

MỤC LỤC

Mục lục	3
Mở đầu	4
1 Kiến thức chuẩn bị về nửa nhóm số	8
1.1. Nửa nhóm số và chiều nhúng của nửa nhóm số	8
1.2. Tập Apéry	10
1.3. Số Frobenius và giống của nửa nhóm số	11
1.4. Số giả Frobenius và kiểu của nửa nhóm số	12
2 Vấn đề Frobenius đối với nửa nhóm số Mersenne	14
2.1. Nửa nhóm số Mersenne và chiều nhúng của nửa nhóm số Mersenne	14
2.2. Tập Apéry của nửa nhóm số Mersenne	19
2.3. Công thức tính số Frobenius, số giả Frobenius, giống và kiểu của nửa nhóm số Mersenne	24
Kết luận	29
Tài liệu tham khảo	30

MỞ ĐẦU

Cho $\mathbb{N}$ là vị nhóm cộng các số tự nhiên. Một *nửa nhóm số* S là một vị nhóm con của $\mathbb{N}$ sao cho phần bù của S trong $\mathbb{N}$ là một tập hợp hữu hạn. Như vậy, S là một nửa nhóm số nếu S là một tập con chứa 0 của $\mathbb{N}$ sao cho $\mathbb{N} \setminus S$ hữu hạn và S đóng kín đối với phép cộng các số tự nhiên.

Cho A là một tập con khác rỗng tùy ý của tập hợp các số tự nhiên $\mathbb{N}$. Ta nói ước chung lớn nhất của A bằng 1, ký hiệu $\gcd(A) = 1$ nếu ước chung lớn nhất của mọi tập con hữu hạn của A đều bằng 1. Ký hiệu $\langle A \rangle$ là tập tất cả các tổ hợp tuyến tính trên $\mathbb{N}$ của A , nghĩa là

$$\langle A \rangle = \{ \lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n \mid \lambda_i \in \mathbb{N}, a_i \in A, n \in \mathbb{N} \}.$$

Chú ý rằng $\langle A \rangle$ là một nửa nhóm số nếu và chỉ nếu $\gcd(A) = 1$.

Cho S là một nửa nhóm số.

(1). Số nguyên lớn nhất không thuộc S được gọi là *số Frobenius* của S và ký hiệu là $F(S)$.

(2). Số nguyên a được gọi là *số giả Frobenius* nếu

$$a \notin S, a + s \in S, \forall s \in S \setminus \{0\}.$$

(3). Tập hợp tất cả các số giả Frobenius được kí hiệu là $PF(S)$.

(4). Lực lượng của tập hợp $PF(S)$ được gọi là *kiểu* của nửa nhóm số S và kí hiệu là $t(S)$.

(5). Lực lượng của tập hợp $\mathbb{N} \setminus S$ được gọi là *giống* của nửa nhóm số S và kí hiệu là $g(S)$.

Các bất biến bằng số nói trên không những cho ta biết thông tin về nửa nhóm số S mà còn cho ta các thông tin liên quan đến việc ứng dụng của lý thuyết nửa nhóm số vào các lĩnh vực khác của toán học như Hình học đại số, Đại số giao hoán, Lý thuyết số,

Khái niệm số Frobenius của một nửa nhóm số xuất phát từ một vấn đề do nhà toán học Frobenius (1849-1917) đưa ra vào cuối thế kỷ 19 và đầu thế kỷ 20. Ông đã đặt vấn đề tìm công thức xác định số nguyên lớn nhất không biểu thị tuyến tính được qua một họ hữu hạn các số nguyên dương nguyên tố cùng nhau với các hệ số nguyên không âm. Vì mỗi nửa nhóm số đều hữu hạn sinh và mỗi phần tử của nửa nhóm số này là một tổ hợp tuyến tính trên $\mathbb{N}$ của hệ sinh, nên vấn đề Frobenius chính là vấn đề xác định công thức tính số Frobenius của một nửa nhóm số. Ngoài việc đặt vấn đề tìm số Frobenius như đã nói thì nhà toán học Frobenius còn đặt ra câu hỏi: có bao nhiêu số nguyên không âm không biểu thị tuyến tính được qua một họ hữu hạn các số nguyên dương nguyên tố cùng nhau với các hệ số nguyên không âm. Điều này có nghĩa là tính giống $g(S)$ của một nửa nhóm số S . Vấn đề Frobenius vẫn chưa được giải quyết trọn vẹn đối với các nửa nhóm số có chiều nhúng lớn hơn hoặc bằng 3.

Một số nguyên dương x được gọi là *số Mersenne* nếu $x = 2^n - 1$ với n là một số nguyên dương nào đó.

Một nửa nhóm số S được gọi là *nửa nhóm số Mersenne* nếu tồn tại một số nguyên dương n sao cho $S = \langle \{2^{n+i} - 1 \mid i \in \mathbb{N}\} \rangle$. Nửa nhóm số Mersenne đó được ký hiệu là $S(n)$.

Trong bài báo [5] trên tạp chí Mathematische Zeitschrift ra năm 2017, J.C. Rosales, M.B. Branco và D. Torráo đã nghiên cứu vấn đề Frobenius đối với nửa nhóm số Mersenne $S(n)$. Họ đã đưa ra công thức tính chiều nhúng, số Frobenius, kiểu và giống của nửa nhóm số sinh bởi các số Mersenne lớn hơn hoặc bằng một số Mersenne cho trước. Họ đã chỉ ra hệ sinh tối tiểu của $S(n)$ là

$\{2^n - 1, 2^{n+1} - 1, \dots, 2^{2n-1} - 1\}$, do đó chiều nhúng của $S(n)$ là $e(S(n)) = n$. Trong [5], các tác giả giải quyết được vấn đề Frobenius đối với nửa nhóm số Mersenne, cụ thể là họ đã chứng minh được rằng $F(S(n)) = 2^{2n} - 2^n - 1$ và $g(S(n)) = 2^{n-1}(2^n + n - 3)$. Ngoài ra, nếu $n \geq 2$ thì bài báo [5] còn chỉ ra

$$PF(S(n)) = \{F(S(n)), F(S(n)) - 1, \dots, F(S(n)) - (n - 2)\}$$

và do đó $t(S(n)) = n - 1$.

Nội dung của luận văn là trình bày lại một cách chi tiết các kết quả trong bài báo nói trên của J.C. Rosales, M. B. Branco và D. Torráo.

Cấu trúc của luận văn được chia thành hai chương, ngoài phần mở đầu, kết luận và tài liệu tham khảo.

Chương 1. Kiến thức chuẩn bị về nửa nhóm số

Trong chương này chúng tôi trình bày một số kiến thức chuẩn bị về nửa nhóm số có liên quan đến nội dung chính của luận văn ở Chương 2, bao gồm những nội dung sau đây:

- 1.1. Nửa nhóm số và chiều nhúng của nửa nhóm số
- 1.2. Tập Apéry
- 1.3. Số Frobenius và giống của nửa nhóm số
- 1.4. Số giả Frobenius và kiểu của nửa nhóm số

Chương 2. Vấn đề Frobenius đối với nửa nhóm số Mersenne

Trong chương này chúng tôi trình bày các kết quả trong bài báo [5] của J.C. Rosales, M. B. Branco và D. Torráo, bao gồm những nội dung sau đây.

- 2.1. Nửa nhóm số Mersenne và chiều nhúng của nửa nhóm số Mersenne
- 2.2. Tập Apéry của nửa nhóm số Mersenne
- 2.3. Công thức tính số Frobenius, số giả Frobenius, giống và kiểu của nửa nhóm số Mersenne

Tác giả xin bày tỏ lòng biết ơn đến cô giáo - PGS.TS. Nguyễn Thị Hồng Loan, cô đã tận tâm giảng dạy, tỉ mỉ hướng dẫn tác giả trong suốt quá trình

hoàn thiện luận văn. Tác giả gửi lời cảm ơn Ban giám hiệu trường THPT Chuyên Lê Quý Đôn - Thành phố Vũng Tàu, các đồng nghiệp tổ Toán, người thân trong gia đình đã tạo mọi điều kiện thuận lợi để tác giả theo học lớp cao học khóa 28. Tác giả xin chân thành cảm ơn các thầy cô trường Đại học Vinh, các thầy cô Khoa Toán, các thầy cô bộ môn Đại số - Lý thuyết số đã nhiệt tình giảng dạy và đã tạo điều kiện tốt nhất cho tác giả trong suốt quá trình học tập.

Trân trọng!

Nghệ An, tháng 06 năm 2022

Tác giả

CHƯƠNG 1

KIẾN THỨC CHUẨN BỊ VỀ NỬA NHÓM SỐ

Trong chương này, chúng tôi trình bày về khái niệm nửa nhóm số, các bất biến của một nửa nhóm số như chiều nhúng, tập Apéry, số Frobenius, giống, số giả Frobenius và kiểu. Đây là những kiến thức chuẩn bị cần dùng cho các chứng minh ở Chương 2. Vì các kiến thức này đã được trình bày chi tiết trong các luận văn trước đây nên chúng tôi chỉ nêu kết quả mà không chứng minh. Các kết quả trong chương này được tham khảo từ các tài liệu [1], [3] và [4].

1.1 Nửa nhóm số và chiều nhúng của nửa nhóm số

1.1.1 Định nghĩa. Cho S là một tập con chứa 0 của tập các số tự nhiên $\mathbb{N}$. Khi đó S được gọi là một *nửa nhóm số* nếu S đóng kín với đối với phép cộng các số tự nhiên và phần bù của S trong $\mathbb{N}$ là tập hữu hạn.

Như vậy, một nửa nhóm số là một vị nhóm con của vị nhóm cộng các số tự nhiên sao cho phần bù của nó trong $\mathbb{N}$ là tập hợp hữu hạn. Nếu $n_1, n_2, \dots, n_p$ là các số nguyên dương sao cho $\gcd(n_1, n_2, \dots, n_p) = 1$ thì tập hợp

$$\langle n_1, n_2, \dots, n_p \rangle = \{n_1\lambda_1 + n_2\lambda_2 + \dots + n_p\lambda_p \mid \lambda_1, \lambda_2, \dots, \lambda_p \in \mathbb{N}\}$$

là một nửa nhóm số. Chú ý rằng, mọi nửa nhóm số đều có dạng này. Khi đó $\{n_1, n_2, \dots, n_p\}$ được gọi là *hệ sinh của nửa nhóm số* $\langle n_1, n_2, \dots, n_p \rangle$.

Cho A là một tập con khác rỗng tùy ý (tập A có thể vô hạn) của tập hợp các số tự nhiên $\mathbb{N}$. Ta nói ước chung lớn nhất của A bằng 1, ký hiệu

$\gcd(A) = 1$ nếu ước chung lớn nhất của mọi tập con hữu hạn của A là 1. Ký hiệu $\langle A \rangle$ là tập tất cả các tổ hợp tuyến tính trên $\mathbb{N}$ của A , nghĩa là

$$\langle A \rangle = \{\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n \mid \lambda_i \in \mathbb{N}, a_i \in A, n \in \mathbb{N}\}.$$

1.1.2 Định lí. Cho A là một tập con khác rỗng của tập hợp các số tự nhiên $\mathbb{N}$. Khi đó $\langle A \rangle$ là một nửa nhóm số nếu và chỉ nếu $\gcd(A) = 1$.

Một hệ sinh của một nửa nhóm số S được gọi là *hệ sinh tối thiểu* nếu mọi tập con thực sự của nó đều không thể sinh ra S .

1.1.3 Mệnh đề. Mỗi nửa nhóm số đều có duy nhất một hệ sinh tối thiểu và hệ sinh tối thiểu này là hữu hạn.

Theo Mệnh đề 1.1.3, mỗi nửa nhóm số đều có duy nhất một hệ sinh tối thiểu và hệ sinh tối thiểu này là hữu hạn. Vì vậy, ta có định nghĩa sau đây.

1.1.4 Định nghĩa. Cho S là một nửa nhóm số và $\{a_1, \dots, a_p\}$ sao cho $a_1 < \dots < a_p$ là một hệ sinh tối thiểu của S . Khi đó:

- *Số bội* của S , kí hiệu là $m(S)$ được định nghĩa là số tự nhiên bé nhất trong hệ sinh tối thiểu của S . Như vậy $m(S) = a_1$.
- *Chiều nhúng* của S , kí hiệu là $e(S)$ được định nghĩa là lực lượng của hệ sinh tối thiểu của S . Do đó $e(S) = p$.

1.1.5 Ví dụ. Cho nửa nhóm số $S = \langle 3, 5, 8 \rangle$ Khi đó ta có:

- $S = \{0, 3, 5, 6, 8 \rightarrow\}$ (trong đó ký hiệu $8 \rightarrow$ nghĩa là các số tự nhiên liên tiếp bắt đầu từ 8).
- $\{3, 5, 8\}$ là một hệ sinh tối thiểu của nửa nhóm số S .
- Chiều nhúng của S là $e(S) = 3$.
- Số bội của S là $m(S) = 3$.

1.2 Tập Apéry

Để nghiên cứu các vấn đề về nửa nhóm số, trước tiên ta tìm hiểu khái niệm tập Apéry.

1.2.1 Định nghĩa. Cho nửa nhóm số S và $n \in S \setminus \{0\}$. Khi đó, tập Apéry của n trong S được xác định như sau:

$$\text{Ap}(S, n) = \{u \in S \mid u - n \notin S\}.$$

1.2.2 Bổ đề. Cho S là một nửa nhóm số và n là một số nguyên dương thuộc S . Nếu $u, v \in S$ sao cho $u + v \in \text{Ap}(S, n)$ thì $\{u, v\} \subseteq \text{Ap}(S, n)$.

1.2.3 Bổ đề. Cho S là một nửa nhóm số và n là một phần tử khác không của S . Khi đó

$$\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n-1)\},$$

trong đó $w(i)$ là phần tử bé nhất của S đồng dư với i theo môđun n với mọi $i \in \{0, 1, \dots, n-1\}$.

1.2.4 Ví dụ. Cho nửa nhóm số $S = \langle 3, 5, 8 \rangle$ Ta có:

$$S = \{0, 3, 5, 6, 8, \dots\}.$$

Ta tính được

$$\text{Ap}(S, 3) = \{0, 5, 10\},$$

$$\text{Ap}(S, 5) = \{0, 3, 6, 9, 12\}.$$

1.2.5 Bổ đề. Cho S là một nửa nhóm số và $n \in S \setminus \{0\}$. Khi đó với mọi $s \in S$, tồn tại duy nhất cặp số $(k, w) \in \mathbb{N} \times \text{Ap}(S, n)$ sao cho

$$s = kn + w.$$

1.2.6 Nhận xét. Từ Bổ đề 1.2.3 và Bổ đề 1.2.5, ta có thể kết luận rằng một số nguyên z thuộc S khi và chỉ khi $z \geq w(z \bmod x)$ (trong đó $z \bmod x$ là số dư của phép chia z cho x).

1.3 Số Frobenius và giống của nửa nhóm số

1.3.1 Định nghĩa. Cho S là một nửa nhóm số. *Số Frobenius* của nửa nhóm số S , ký hiệu $F(S)$ được định nghĩa là số nguyên lớn nhất không thuộc S .

Như vậy

$$F(S) = \max(\mathbb{Z} \setminus S).$$

1.3.2 Ví dụ. 1). Cho nửa nhóm số $S = \langle 3, 5, 8 \rangle = \{0, 3, 5, 6, 8 \rightarrow\}$. Khi đó

$$F(S) = 7.$$

2). Cho nửa nhóm số $S = \langle 4, 7 \rangle$. Khi đó

$$S = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18 \rightarrow\}$$

và như vậy $F(S) = 17$.

1.3.3 Định nghĩa. Cho S là một nửa nhóm số. Ta ký hiệu phần bù của S trong $\mathbb{N}$ là $H(S)$ thì tập hợp $H(S)$ là hữu hạn. *Giống* của nửa nhóm số S , ký hiệu là $g(S)$ được định nghĩa là lực lượng của tập $H(S)$.

1.3.4 Ví dụ. 1). Xét nửa nhóm số

$$S = \langle 3, 5, 8 \rangle = \{0, 3, 5, 6, 8 \rightarrow\}.$$

Khi đó $H(S) = \{1, 2, 4, 7\}$, do đó $g(S) = 4$.

2). Xét nửa nhóm số

$$S = \langle 3, 8 \rangle = \{0, 3, 6, 8, 9, 11, 12, 14 \rightarrow\}.$$

Khi đó ta tính được $g(S) = 7$.

Kết quả sau cho thấy số Frobenius và giống của một nửa nhóm số có thể xác định được qua tập Apéry.

1.3.5 Bổ đề. Cho S là một nửa nhóm số và n là một phần tử khác 0 của S .

Khi đó:

$$(1). F(S) = (\max \text{Ap}(S, n)) - n,$$

$$(2). g(S) = \frac{1}{n} \left(\sum_{w \in \text{Ap}(S, n)} w \right) - \frac{n-1}{2}.$$

Nếu $S = \langle x, y \rangle$ là một nửa nhóm số với hệ sinh tối thiểu là $\{x, y\}$ thì

$$\text{Ap}(S, x) = \{0, y, 2y, \dots, (x-1)y\}$$

và do đó từ Bổ đề 1.3.5 ta có hệ quả sau. Đây chính là kết quả của Sylvester từ năm 1882, giải quyết vấn đề Frobenius trong trường hợp chiều nhúng của nửa nhóm số bằng 2.

1.3.6 Hệ quả. Cho x và y là hai số nguyên không âm sao cho $\gcd(x, y) = 1$.

Khi đó ta có:

$$(1). F(\langle x, y \rangle) = xy - x - y,$$

$$(2). g(\langle x, y \rangle) = \frac{xy - x - y + 1}{2}.$$

1.4 Số giả Frobenius và kiểu của nửa nhóm số

1.4.1 Định nghĩa. Cho S là một nửa nhóm số.

(1). Số nguyên u được gọi là *số giả Frobenius* nếu

$$u \notin S, u + s \in S, \forall s \in S \setminus \{0\}.$$

(2). Tập hợp tất cả các số giả Frobenius được kí hiệu là $\text{PF}(S)$.

(3). *Kiểu* của nửa nhóm số S , kí hiệu là $t(S)$ được định nghĩa là lực lượng của tập hợp $\text{PF}(S)$.

1.4.2 Nhận xét. Từ Định nghĩa 1.4.1, ta có nhận xét sau đây.

(1). $\text{PF}(S) = \{u \in \mathbb{Z} \setminus S \mid u + s \in S, \forall s \in S\}$ và là tập hữu hạn. Thật vậy, nếu $S \neq \mathbb{N}$ thì $\text{PF}(S) \subseteq \mathbb{N} \setminus S$ mà $\mathbb{N} \setminus S$ là tập hữu hạn.

(2). $F(S) \in PF(S)$ và $F(S)$ là số lớn nhất trong tập hợp các số giả Frobenius $PF(S)$.

(3). Cho S là một nửa nhóm số. Trên tập hợp các số nguyên $\mathbb{Z}$ ta định nghĩa một quan hệ hai ngôi " $\leq_S$ " như sau:

$$u \leq_S v \text{ nếu } v - u \in S.$$

Quan hệ này có tính phản xạ, tính phản đối xứng và bắc cầu. Do đó " $\leq_S$ " là một quan hệ thứ tự trên tập hợp các số nguyên $\mathbb{Z}$.

Cho $X \subseteq \mathbb{Z}$. Ta ký hiệu $Maximal_{\leq_S}(X)$ là tập tất cả các phần tử cực đại của X theo quan hệ thứ tự $\leq_S$.

1.4.3 Mệnh đề. Cho S là một nửa nhóm số. Khi đó:

- (1). $PF(S) = Maximal_{\leq_S}(\mathbb{Z} \setminus S)$,
- (2). $x \in \mathbb{Z} \setminus S$ nếu và chỉ nếu $h - x \in S$ với $h \in PF(S)$.

Vì tập hợp $Minimal_{\leq_S}(S \setminus \{0\})$ chính là hệ sinh tối tiểu của nửa nhóm số S nên Mệnh đề 1.4.3 cho ta một sự đối ngẫu giữa hệ sinh tối tiểu của S và tập các số giả Frobenius của S .

1.4.4 Bổ đề. Cho S là một nửa nhóm số và n là một phần tử khác 0 của S . Khi đó

$$PF(S) = \{w - n \mid w \in Maximal_{\leq_S}(Ap(S, n))\}.$$

CHƯƠNG 2

VẤN ĐỀ FROBENIUS ĐỐI VỚI NỬA NHÓM SỐ MERSENNE

Như đã nói trong Mở đầu, vấn đề Frobenius đến nay vẫn chưa có câu trả lời trọn vẹn đối với các nửa nhóm số có chiều nhúng lớn hơn hoặc bằng 3. Vì thế các nhà toán học có xu hướng giải quyết vấn đề này đối với một số lớp nửa nhóm số đặc biệt.

Trong [5], J.C. Rosales, M.B. Branco và D. Torrão đã nghiên cứu vấn đề Frobenius đối với nửa nhóm số Mersenne $S(n)$. Chương này, chúng tôi trình bày chi tiết các kết quả trong [5].

2.1 Nửa nhóm số Mersenne và chiều nhúng của nửa nhóm số Mersenne

2.1.1 Định nghĩa. Một số nguyên dương x được gọi là *số Mersenne* nếu $x = 2^n - 1$ với n là một số nguyên dương nào đó.

Cho A là một tập con khác rỗng của $\mathbb{N}$. Ký hiệu $\langle A \rangle$ là vị nhóm con của vị nhóm cộng các số tự nhiên $\mathbb{N}$ sinh bởi A , nghĩa là

$$\langle A \rangle = \{ \lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n \mid \lambda_i \in \mathbb{N}, a_i \in A, n \in \mathbb{N} \}.$$

Chú ý rằng $\langle A \rangle$ là nửa nhóm số khi và chỉ khi $\gcd(A) = 1$.

2.1.2 Bổ đề. Cho A là tập hợp khác rỗng các số nguyên dương và $M = \langle A \rangle$. Các điều kiện sau là tương đương:

- (1). $2a + 1 \in M$ với mọi $a \in A$;

(2). $2m + 1 \in M$ với mọi $m \in M \setminus \{0\}$.

Chứng minh. (1) $\Rightarrow$ (2). Nếu $m \in M \setminus \{0\}$, thì tồn tại $a_1, \dots, a_k \in A$ sao cho

$$m = a_1 + \dots + a_k.$$

Nếu $k = 1$ thì $m = a_1$ và do đó $2m + 1 = 2a_1 + 1 \in M$.

Nếu $k \geq 2$ thì

$$2m + 1 = 2(a_1 + \dots + a_{k-1}) + 2a_k + 1 \in M,$$

vì M đóng kín đối với phép cộng.

(2) $\Rightarrow$ (1). Hiển nhiên. □

Cho n là một số nguyên dương. Ký hiệu $S(n) = \langle \{2^{n+i} - 1 \mid i \in \mathbb{N}\} \rangle$ là vị nhóm con của vị nhóm cộng các số tự nhiên $\mathbb{N}$ sinh bởi tập $\{2^{n+i} - 1 \mid i \in \mathbb{N}\}$. Mệnh đề sau đây cho thấy $S(n)$ là một nửa nhóm số.

2.1.3 Mệnh đề. *Cho n là một số nguyên dương. Khi đó $S(n)$ là một nửa nhóm số. Hơn nữa, $2s + 1 \in S(n)$ với mọi $s \in S(n) \setminus \{0\}$.*

Chứng minh. Rõ ràng, $S(1) = \mathbb{N}$ là một nửa nhóm số và với mọi $s \in \mathbb{N} \setminus \{0\}$, ta có $2s + 1 \in \mathbb{N}$.

Giả sử $n \geq 2$ và ta chứng tỏ rằng $S(n)$ là một nửa nhóm số. Vì $S(n)$ là một vị nhóm con của vị nhóm cộng các số tự nhiên $(\mathbb{N}, +)$ nên chỉ cần chứng minh $\mathbb{N} \setminus S(n)$ là tập hữu hạn, điều này tương đương với việc chứng tỏ rằng $\gcd(S(n)) = 1$.

Thật vậy, vì $2^n - 1$ và $2^{n+1} - 1$ đều thuộc $S(n)$ nên

$$\gcd\{2^n - 1, 2^{n+1} - 1\} = \gcd\{2^n - 1, 2(2^n - 1) + 1\} = 1.$$

Ta có

$$S(n) = \langle \{2^{n+i} - 1 \mid i \in \mathbb{N}\} \rangle.$$

Nếu $i \in \mathbb{N}$ thì

$$2(2^{n+i} - 1) + 1 = 2^{n+i+1} - 1 \in S(n).$$

Theo Bổ đề 2.1.2, ta có $2s + 1 \in S(n)$ với mọi $s \in S(n) \setminus \{0\}$.

□

2.1.4 Định nghĩa. Một nửa nhóm số S được gọi là *nửa nhóm số Mersenne* nếu tồn tại một số nguyên dương n sao cho $S = S(n)$.

Như vậy, các nửa nhóm số Mersenne là các nửa nhóm số có dạng $S(n)$ với n là một số nguyên dương nào đó.

Bây giờ chúng ta sẽ tìm hiểu về hệ sinh tối tiểu của nửa nhóm số Mersenne. Trước hết ta có bổ đề sau.

2.1.5 Bổ đề. Cho n là một số nguyên dương và cho

$$S = \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\} \rangle.$$

Khi đó $2s + 1 \in S$ với mọi $s \in S \setminus \{0\}$.

Chứng minh. Nếu $n = 1$ thì $S = \mathbb{N}$ và bổ đề là đúng trong trường hợp này. Giả sử $n \geq 2$. Nếu $i \in \{0, 1, \dots, n-2\}$, thì

$$2(2^{n+i} - 1) + 1 = 2^{n+i+1} - 1 \in S.$$

Ngoài ra

$$2(2^{2n-1} - 1) + 1 = 2^{2n} - 1 = (2^n - 1)(2^n + 1) \in S.$$

Bằng cách áp dụng Bổ đề 2.1.2, ta thu được $2s + 1 \in S$ với mọi $s \in S \setminus \{0\}$.

□

Cho X và Y là các tập hợp khác rỗng các số nguyên dương sao cho $Y \subseteq X$ và $X \subseteq \langle Y \rangle$. Khi đó $\langle X \rangle = \langle Y \rangle$. Mệnh đề sau chỉ ra một hệ sinh hữu hạn của nửa nhóm số Mersenne.

2.1.6 Mệnh đề. Nếu n là số nguyên dương thì

$$S(n) = \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\} \rangle.$$

Chứng minh. Cho $S = \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\} \rangle$

Ta cần chứng minh $S(n) = S$. Theo nhận xét trên đây, một tập con của một nửa nhóm mà chứa một tập sinh của nửa nhóm đó thì tập hợp đó cũng chính là tập sinh của nửa nhóm đó. Vì vậy, ta chỉ cần chứng minh $2^{n+i} - 1 \in S$ với mọi $i \in \mathbb{N}$.

Thật vậy, ta sử dụng quy nạp theo i .

Với $i = 0$, khẳng định đúng. Giả sử rằng khẳng định đúng với i và ta chứng minh khẳng định đúng với $i + 1$. Ta có

$$2^{n+i+1} - 1 = 2(2^{n+i} - 1) + 1,$$

do đó, theo giả thiết quy nạp và Bổ đề 2.1.5 ta có $2^{n+i+1} - 1 \in S$. $\square$

Mệnh đề trên cho ta thấy $\{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\}$ là một hệ sinh của nửa nhóm số Mersenne $S(n)$.

2.1.7 Bổ đề. Cho n là một số nguyên lớn hơn hoặc bằng 2. Khi đó

$$2^{2n-1} - 1 \notin \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-2\}\} \rangle.$$

Chứng minh. Giả sử ngược lại rằng tồn tại $a_0, \dots, a_{n-2} \in \mathbb{N}$ sao cho

$$2^{2n-1} - 1 = a_0(2^n - 1) + \dots + a_{n-2}(2^{2n-2} - 1).$$

Khi đó

$$2^{2n-1} - 1 = a_0 2^n + \dots + a_{n-2} 2^{2n-2} - (a_0 + \dots + a_{n-2})$$

và suy ra

$$(a_0 + \dots + a_{n-2}) \equiv 1 \pmod{2^n}.$$

Do đó $(a_0 + \dots + a_{n-2}) = 1 + 2^n k$ với $k \in \mathbb{N}$.

Nếu $k = 0$ thì $a_0 + \dots + a_{n-2} = 1$ và do đó tồn tại $i \in \{0, 1, \dots, n-2\}$ sao cho $a_i = 1$ và $a_j = 0$ với mọi $j \in \{0, 1, \dots, n-2\} \setminus \{i\}$. Vì vậy, ta suy ra rằng $2^{2^{n-1}} - 1 = 2^{n+i} - 1$ với $i \in \{0, 1, \dots, n-2\}$, điều này là vô lý.

Nếu $k \neq 0$ thì $a_0 + \dots + a_{n-2} \geq 1 + 2^n$. Điều này suy ra rằng

$$\begin{aligned} a_0(2^n - 1) + \dots + a_{n-2}(2^{2^{n-2}} - 1) &\geq (a_0 + \dots + a_{n-2})(2^n - 1) \\ &\geq (1 + 2^n)(2^n - 1) \\ &= 2^{2^n} - 1 \\ &> 2^{2^{n-1}} - 1. \end{aligned}$$

Điều này là vô lý. Vậy bổ đề đã được chứng minh. □

Định lý sau đây chỉ ra hệ sinh tối tiểu của nửa nhóm số Mersenne.

2.1.8 Định lí. *Cho n là một số nguyên dương và $S(n)$ là nửa nhóm số Mersenne liên kết với n . Khi đó chiều nhúng của $S(n)$ là $e(S(n)) = n$. Hơn nữa $\{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\}$ là hệ sinh tối tiểu của $S(n)$.*

Chứng minh. Với $n = 1$ thì định lý hiển nhiên đúng.

Giả sử $n \geq 2$. Theo Mệnh đề 2.1.6,

$$\{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\}$$

là một hệ sinh của $S(n)$. Nếu nó không phải là hệ sinh tối tiểu thì tồn tại $h \in \{1, \dots, n-1\}$ sao cho

$$2^{n+h} - 1 \in \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, h-1\}\} \rangle.$$

Ký hiệu

$$S = \langle \{2^{n+i} - 1 \mid i \in \{0, 1, \dots, h-1\}\} \rangle.$$

Nếu $i \in \{0, 1, \dots, h-2\}$ thì $2(2^{n+i} - 1) + 1 = 2^{n+i+1} - 1 \in S$. Hơn nữa

$$2(2^{n+h-1} - 1) + 1 = 2^{n+h} - 1 \in S.$$

Áp dụng Bổ đề 2.1.2, ta có $2s + 1 \in S$ với mọi $s \in S \setminus \{0\}$.

Bây giờ chúng ta sử dụng quy nạp theo i để chứng minh rằng $2^{n+i} - 1 \in S$ với mọi $i \in \mathbb{N}$.

Với $i = 0$ thì khẳng định là đúng. Giả sử khẳng định đúng với i và ta sẽ chứng minh khẳng định đúng với $i + 1$. Thật vậy, vì

$$2^{n+i+1} - 1 = 2(2^{n+i} - 1) + 1$$

nên áp dụng giả thiết quy nạp và $2s + 1 \in S$ với mọi $s \in S \setminus \{0\}$, ta thu được

$$2^{n+i+1} - 1 \in S.$$

Do đó $2^{2n-1} - 1 \in S$, điều này mâu thuẫn với Bổ đề 2.1.7.

Những phân tích trên đã chứng tỏ

$$\{2^{n+i} - 1 \mid i \in \{0, 1, \dots, n-1\}\}$$

là hệ sinh tối tiểu của $S(n)$ và định lý được chứng minh. □

Từ các kết quả trong phần này, chúng ta thấy rằng với mỗi số nguyên dương n tồn tại duy nhất một nửa nhóm số Mersenne với chiều nhúng n .

Chẳng hạn

$$S(4) = \langle \{2^4 - 1, 2^5 - 1, 2^6 - 1, 2^7 - 1\} \rangle = \langle \{15, 31, 63, 127\} \rangle$$

là nửa nhóm số Mersenne duy nhất với chiều nhúng 4.

2.2 Tập Apéry của nửa nhóm số Mersenne

Cho u là một phần tử khác 0 của nửa nhóm số S . Trong Chương 1, ta đã định nghĩa tập Apéry của u trong S là

$$Ap(S, u) = \{s \in S \mid s - u \notin S\}.$$

Tập $Ap(S, u)$ cho ta nhiều thông tin về nửa nhóm số S .

Trong phần này ta sẽ mô tả tập $Ap(S(n), 2^n - 1)$. Để thuận tiện, từ bây giờ ta sẽ ký hiệu các phần tử $2^{n+i} - 1$ bởi s_i với mỗi $i \in \{0, 1, \dots, n-1\}$. Vì vậy, với ký hiệu này, ta có $\{s_0, s_1, \dots, s_{n-1}\}$ là hệ sinh tối tiểu của $S(n)$. Ta có các đẳng thức sau đây.

2.2.1 Bổ đề. *Cho n là số nguyên lớn hơn hoặc bằng 2. Khi đó:*

- (1) nếu $0 < i \leq j < n-1$ thì $s_i + 2s_j = 2s_{i-1} + s_{j+1}$;
- (2) nếu $0 < i \leq n-1$ thì $s_i + 2s_{n-1} = 2s_{i-1} + (2^n + 1)s_0$.

Chứng minh. (1) Ta có

$$\begin{aligned} s_i + 2s_j &= (2^{n+i} - 1) + 2(2^{n+j} - 1) \\ &= 2^{n+i} + 2^{n+j+1} - 3 \\ &= 2(2^{n+i-1} - 1) + 2^{n+j+1} - 1 \\ &= 2s_{i-1} + s_{j+1}. \end{aligned}$$

(2) Ta có

$$\begin{aligned} s_i + 2s_{n-1} &= (2^{n+i} - 1) + 2(2^{n+n-1} - 1) \\ &= 2(2^{n+i-1} - 1) + (2^{2n} - 1) \\ &= 2(2^{n+i-1} - 1) + (2^n + 1)(2^n - 1) \\ &= 2s_{i-1} + (2^n + 1)s_0. \end{aligned}$$

□

2.2.2 Định nghĩa. Ta nói rằng dãy $(a_1, \dots, a_k)$ là một k - bộ số dư nếu nó thỏa mãn các điều kiện sau:

- (1) với mọi $i \in \{1, \dots, k\}$ ta có $a_i \in \{0, 1, 2\}$;
- (2) nếu $i \in \{2, \dots, k\}$ và $a_i = 2$ thì $a_1 = \dots = a_{i-1} = 0$.

2.2.3 Bổ đề. *Cho n là số nguyên lớn hơn hoặc bằng 2. Nếu $x \in Ap(S(n), s_0)$ thì tồn tại một $(n-1)$ - bộ số dư $(a_1, \dots, a_{n-1})$ sao cho*

$$x = a_1s_1 + \dots + a_{n-1}s_{n-1}.$$

Chứng minh. Chứng minh bằng quy nạp theo x .

Bổ đề là rõ ràng với $x = 0$. Giả sử rằng $x > 0$ và gọi

$$j = \min \{i \in \{0, \dots, n-1\} \mid x - s_i \in S(n)\}.$$

Nhận xét rằng $j \neq 0$ vì $x \in Ap(S(n), s_0)$. Theo quy nạp, tồn tại một $(n-1)$ -bộ số dư $(a_1, \dots, a_{n-1})$ sao cho $x - s_j = a_1 s_1 + \dots + a_{n-1} s_{n-1}$. Do đó

$$x = a_1 s_1 + \dots + (a_j + 1) s_j + \dots + a_{n-1} s_{n-1}.$$

Để kết thúc chứng minh, ta chỉ cần chứng tỏ $(a_1, \dots, a_j + 1, \dots, a_{n-1})$ là một $(n-1)$ -bộ số dư. Nếu $a_j + 1 = 3$ thì bằng cách áp dụng Bổ đề 2.2.1, ta nhận được

$$(a_j + 1) s_j = 3s_j = 2s_{j-1} + s_{j+1}$$

trong trường hợp $j < n-1$ hoặc

$$(a_j + 1) s_j = 3s_j = 2s_{j-1} + (2^n + 1) s_0$$

trong trường hợp $j = n-1$. Trong cả hai trường hợp, đều dẫn đến

$$x - s_{j-1} \in S(n),$$

mâu thuẫn với tính tối thiểu của j .

Nếu tồn tại $k > j$ sao cho $a_k = 2$, sử dụng Bổ đề 2.2.1, ta thu được hoặc

$$s_j + 2s_k = 2s_{j-1} + s_{k+1}$$

trong trường hợp $k < n-1$ hoặc

$$s_j + 2s_k = 2s_{j-1} + (2^n + 1) s_0$$

trong trường hợp $k = n-1$. Trong cả hai trường hợp, một lần nữa ta nhận thấy rằng

$$x - s_{j-1} \in S(n),$$

mâu thuẫn với tính tối tiểu của j .

Bây giờ, lại do tính tối tiểu của j , ta có

$$a_1 = \dots = a_{j-1} = 0$$

và vì vậy $(a_1, \dots, a_j + 1, \dots, a_{n-1})$ là $(n-1)$ - bộ số dư.

Vậy bổ đề được chứng minh. □

Lưu ý rằng nếu h là một số nguyên dương thì dãy số

$$2^n, 2^{n+1}, \dots, 2^{n+h}$$

là một cấp số nhân với công bội bằng 2 và do đó tổng các số hạng của nó là

$$2^n + 2^{n+1} + \dots + 2^{n+h} = 2^{n+h+1} - 2^n.$$

2.2.4 Định lí. Cho n là số nguyên lớn hơn hoặc bằng 2 và $S(n)$ là nửa nhóm số Mersenne với hệ sinh tối tiểu $\{s_0, s_1, \dots, s_{n-1}\}$. Khi đó

$$Ap(S(n), s_0) = \{a_1 s_1 + \dots + a_{n-1} s_{n-1} \mid (a_1, \dots, a_{n-1}) \text{ là một } (n-1) - \text{bộ số dư}\}.$$

Chứng minh. Ký hiệu R là tập hợp tất cả các $(n-1)$ - bộ số dư. Rõ ràng

$$\begin{aligned} R &= \{0, 1\}^{n-1} \cup \{(a_1, \dots, a_{n-1}) \in R \mid a_1 = 2\} \\ &\quad \cup \dots \cup \{(a_1, \dots, a_{n-1}) \in R \mid a_{n-1} = 2\}. \end{aligned}$$

Để ý rằng R là hợp của các tập rời rạc, do đó, lực lượng của R bằng

$$2^{n-1} + 2^{n-2} + \dots + 2^0 = 2^n - 1 = s_0.$$

Theo Bổ đề 2.2.3, ta biết rằng

$$Ap(S(n), s_0) \subseteq \{a_1 s_1 + \dots + a_{n-1} s_{n-1} \mid (a_1, \dots, a_{n-1}) \in R\}.$$

Ngoài ra, theo lý luận trên, chúng ta nhận thấy rằng lực lượng của tập hợp

$$\{a_1 s_1 + \dots + a_{n-1} s_{n-1} \mid (a_1, \dots, a_{n-1}) \in R\}$$

nhỏ hơn hoặc bằng s_0 .

Theo Bổ đề 1.2.3, lực lượng của $Ap(S(n), s_0)$ bằng s_0 , và do đó

$$Ap(S(n), s_0) = \{a_1s_1 + \dots + a_{n-1}s_{n-1} \mid (a_1, \dots, a_{n-1}) \in R\}.$$

□

Từ chứng minh của định lý trên ta có ngay hệ quả sau.

2.2.5 Hệ quả. Cho n là số nguyên lớn hơn hoặc bằng 2, $(a_1, \dots, a_{n-1})$ và $(b_1, \dots, b_{n-1})$ là các $(n-1)$ - bộ số dư phân biệt. Khi đó ta có

$$a_1s_1 + \dots + a_{n-1}s_{n-1} \neq b_1b_1 + \dots + b_{n-1}b_{n-1}.$$

Sau đây là một ví dụ minh họa cho Định lý 2.2.4.

2.2.6 Ví dụ. Tính $Ap(S(4), s_0)$.

- Ta có $s_0 = 15$ và $S(4) = \langle \{15, 31, 63, 127\} \rangle$.
- Các 3 - bộ số dư là $(0, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, $(0, 1, 1)$, $(1, 0, 0)$, $(1, 1, 0)$, $(1, 0, 1)$, $(1, 1, 1)$, $(2, 0, 0)$, $(2, 1, 0)$, $(2, 0, 1)$, $(2, 1, 1)$, $(0, 2, 0)$, $(0, 2, 1)$ và $(0, 0, 2)$.
- Vì $s_1 = 31$, $s_2 = 63$ và $s_3 = 127$, theo Định lý 2.2.4 ta thu được $Ap(S(4), s_0) = \{0, 63, 127, 190, 31, 94, 158, 221, 62, 125, 189, 252, 126, 253, 254\}$.

Ví dụ tiếp theo, ta áp dụng Nhận xét 1.2.6 để xét xem một số nguyên dương có thuộc hay không thuộc $S(4)$.

2.2.7 Ví dụ. Từ Ví dụ 2.2.6, ta có

$$\begin{aligned} Ap(S(4), s_0) = \{w(0) = 0, w(1) = 31, w(2) = 62, w(3) = 63, w(4) = 94, \\ w(5) = 125, w(6) = 126, w(7) = 127, w(8) = 158, w(9) = 189, w(10) = \\ 190, w(11) = 221, w(12) = 252, w(13) = 253, w(14) = 254\} \end{aligned}$$

Từ đó ta thấy rằng $172 \in S(4)$ và $222 \notin S(4)$, bởi vì $172 \geq w(172 \bmod 15) = w(7) = 127$ và $222 < w(222 \bmod 15) = w(12) = 252$.

2.3 Công thức tính số Frobenius, số giả Frobenius, giống và kiểu của nửa nhóm số Mersenne

2.3.1 Bổ đề. Cho n là số nguyên lớn hơn hoặc bằng 2 và R là tập hợp tất cả các $(n-1)$ - bộ số dư. Khi đó, các phần tử cực đại (theo thứ tự tích) trong R là

$$(2, 1, \dots, 1), (0, 2, 1, \dots, 1), \dots, (0, 0, \dots, 2).$$

Trong kết quả sau đây, chúng ta sẽ thấy rằng

$$2s_1 + s_2 + \dots + s_{n-1}, 2s_2 + s_3 + \dots + s_{n-1}, \dots, 2s_{n-1}$$

là một dãy các số nguyên, trong đó mỗi số hạng có được bằng cách lấy số ngay trước nó cộng thêm 1.

2.3.2 Bổ đề. Cho n là số nguyên lớn hơn hoặc bằng 3 và cho $i \in \{1, \dots, n-2\}$. Khi đó

$$2s_i + s_{i+1} + \dots + s_{n-1} + 1 = 2s_{i+1} + s_{i+2} + \dots + s_{n-1}.$$

Chứng minh. Điều này tương đương với chứng minh rằng $2s_i + 1 = s_{i+1}$. Nhưng điều này là rõ ràng, bởi vì $2(2^{n+i} - 1) + 1 = 2^{n+i+1} - 1$.

□

Định lý sau đây đưa ra công thức tính số Frobenius của nửa nhóm số Mersenne.

2.3.3 Định lí. Cho n là số nguyên lớn hơn hoặc bằng 2 và $S(n)$ là nửa nhóm số Mersenne liên kết với n . Khi đó

$$F(S(n)) = 2^{2n} - 2^n - 1.$$

Chứng minh. Bằng cách áp dụng Định lý 2.2.4, Bổ đề 2.3.1 và 2.3.2, ta suy ra rằng

$$\text{Max}(Ap(S(n), s_0)) = 2s_{n-1}.$$

Sử dụng Bổ đề 1.3.5, ta có

$$F(S(n)) = 2s_{n-1} - s_0 = 2(2^{2^{n-1}} - 1) - (2^n - 1) = 2^{2^n} - 2^n - 1.$$

□

Định lý sau đây cho ta thông tin về kiểu và số giả Frobenius của nửa nhóm số Mersenne.

2.3.4 Định lý. *Cho n là số nguyên lớn hơn hoặc bằng 2 và $S(n)$ là nửa nhóm số Mersenne liên kết với n . Khi đó $t(S(n)) = n - 1$. Hơn nữa*

$$PF(S(n)) = \{F(S(n)), F(S(n)) - 1, \dots, F(S(n)) - (n - 2)\}.$$

Chứng minh. Từ Định lý 2.2.4 và Bổ đề 2.3.1, ta suy ra rằng

$$\text{Maximal}_{\leq S(n)} Ap(S(n), s_0) \subseteq \{2s_1 + \dots + s_{n-1}, 2s_2 + \dots + s_{n-1}, \dots, 2s_{n-1}\}.$$

Bằng cách sử dụng Bổ đề 2.3.2, ta có các phần tử trong tập hợp này là các số nguyên dương liên tiếp và do đó hiệu số giữa hai phần tử bất kỳ của nó nhỏ hoặc bằng $n - 2$. Vì $2^n - 1$ là số nguyên dương nhỏ nhất trong $S(n)$ và $2^n - 1 > n - 2$ nên hiệu giữa hai phần tử phân biệt của

$$\{2s_1 + s_2 + \dots + s_{n-1}, 2s_2 + s_3 + \dots + s_{n-1}, \dots, 2s_{n-1}\}$$

không thuộc $S(n)$. Do đó

$$\text{Maximal}_{\leq S(n)} Ap(S(n), s_0) = \{2s_1 + \dots + s_{n-1}, 2s_2 + \dots + s_{n-1}, \dots, 2s_{n-1}\}.$$

Theo chứng minh của Định lý 2.3.3, ta có

$$F(S(n)) = 2s_{n-1} - s_0.$$

Từ Bổ đề 2.3.2, ta nhận được

$$\begin{aligned} \text{Maximal}_{\leq S(n)} Ap(S(n), s_0) = \\ \{F(S(n)) + s_0, F(S(n)) + s_0 - 1, \dots, F(S(n)) + s_0 - (n - 2)\} \end{aligned}$$

Cuối cùng, theo Bổ đề 1.4.4, chúng ta thu được

$$PF(S(n)) = \{F(S(n)), F(S(n)) - 1, \dots, F(S(n)) - (n - 2)\}.$$

□

Chú ý rằng định lý trên không đúng với $n = 1$, vì

$$S(1) = \mathbb{N}, PF(S(1)) = \{-1\}$$

và do đó $t(S(1)) = 1$.

Định lý sau cho ta công thức tính giống của nửa nhóm số Mersenne.

2.3.5 Định lí. *Cho n là một số nguyên dương và $S(n)$ là nửa nhóm số Mersenne liên kết với n . Khi đó*

$$g(S(n)) = 2^{n-1} (2^n + n - 3).$$

Chứng minh. Với $n = 1$, định lý là hiển nhiên đúng. Giả sử rằng $n \geq 2$ và gọi R là tập hợp tất cả các $(n - 1)$ - bộ số dư. Bằng cách áp dụng Bổ đề 1.3.5, Định lý 2.2.4 và Hệ quả 2.2.5, chúng ta có

$$g(S(n)) = \frac{1}{s_0} \left(\sum_{(a_1, \dots, a_{n-1}) \in R} a_1 s_1 + \dots + a_{n-1} s_{n-1} \right) - \frac{s_0 - 1}{2}.$$

Rõ ràng là

$$\begin{aligned} \sum_{(a_1, \dots, a_{n-1}) \in R} a_1 s_1 + \dots + a_{n-1} s_{n-1} &= \sum_{(a_1, \dots, a_{n-1}) \in R, a_1=1} s_1 \\ &+ \sum_{(a_1, \dots, a_{n-1}) \in R, a_1=2} 2s_1 + \dots + \sum_{(a_1, \dots, a_{n-1}) \in R, a_{n-1}=1} s_{n-1} \\ &+ \sum_{(a_1, \dots, a_{n-1}) \in R, a_{n-1}=2} 2s_{n-1}. \end{aligned}$$

Với $i \in \{1, \dots, n - 1\}$. Ta có:

- Lực lượng của tập hợp $\{(a_1, \dots, a_{n-1}) \in R \mid a_i = 2\}$ là 2^{n-1-i} ;

- Lực lượng của tập hợp $\{(a_1, \dots, a_{n-1}) \in R \mid a_i = 1 \text{ và } 2 \notin \{a_1, \dots, a_{i-1}\}\}$ là 2^{n-2} ;

- Nếu $1 \leq j < i$ thì lực lượng của tập hợp $\{(a_1, \dots, a_{n-1}) \in R \mid a_i = 1 \text{ và } a_j = 2\}$ là 2^{n-j-2} ;

Khi đó ta suy ra rằng

$$\begin{aligned}
& \sum_{(a_1, \dots, a_{n-1}) \in R} a_1 s_1 + \dots + a_{n-1} s_{n-1} \\
&= \sum_{i=1}^{n-1} (2^{n-2} + 2^{n-3} + \dots + 2^{n-1-i}) s_i + \sum_{i=1}^{n-1} 2^{n-1-i} 2 s_i \\
&= \sum_{i=1}^{n-1} (2^{n-1} - 2^{n-1-i}) s_i + \sum_{i=1}^{n-1} 2^{n-i} s_i \\
&= \sum_{i=1}^{n-1} (2^{n-1} - 2^{n-1-i} + 2^{n-i}) s_i \\
&= \sum_{i=1}^{n-1} (2^{n-1} + 2^{n-1-i}) s_i \\
&= \sum_{i=1}^{n-1} (2^{n-1} + 2^{n-1-i}) (2^{n+i} - 1) \\
&= \sum_{i=1}^{n-1} (2^{2n+i-1} + 2^{2n-1} - 2^{n-1} - 2^{n-1-i}) \\
&= 2^{3n-1} - 2^{2n} + (n-1) 2^{2n-1} - (n-1) 2^{n-1} - (2^{n-1} - 1) \\
&= 2^{3n-1} - 2^{2n} + (n-1) 2^{2n-1} - n 2^{n-1} + 1 \\
&= (2^n - 1) (2^{2n-1} - 2^n + n 2^{n-1} - 1).
\end{aligned}$$

Do đó ta nhận được

$$\begin{aligned}
g(S(n)) &= 2^{2n-1} - 2^n + n2^{n-1} - 1 - \frac{2^n - 2}{2} \\
&= 2^{2n-1} - 2^n + (n-1)2^{n-1} \\
&= 2^{n-1}(2^n + n - 3).
\end{aligned}$$

□

Ví dụ sau đây sẽ minh họa cho các định lý 2.3.3, 2.3.4, và 2.3.5

2.3.6 Ví dụ. Tính số Frobenius, kiểu và giống của nửa nhóm số Mersenne $S(4)$.

- Từ Định lý 2.3.3, ta thu được $FS(4) = 2^8 - 2^4 - 1 = 239$.
- Theo Định lý 2.3.4, ta có $t(S(4)) = 3$ và $PF(S(4)) = \{239, 238, 237\}$.
- Áp dụng Định lý 2.3.5 ta có $g(S(4)) = 2^3(2^4 + 4 - 3) = 136$.

KẾT LUẬN

Nội dung chính của luận văn là trình bày về nửa nhóm số Mersenne và một số bất biến của nửa nhóm số Mersenne. Dựa vào bài báo [5] của J.C. Rosales, M. B. Branco, D. Torráo và các tài liệu tham khảo liên quan, chúng tôi đã trình bày được những nội dung chính sau đây.

1. Một số kiến thức chuẩn bị về nửa nhóm số có liên quan đến nội dung chính của luận văn (các mục 1.1, 1.2, 1.3, 1.4).
2. Khái niệm và một số tính chất của nửa nhóm số Mersenne, chiều nhúng của nửa nhóm số Mersenne, tập Apéry của nửa nhóm số Mersenne (các mục 2.1, 2.2).
3. Các công thức tính số Frobenius $F(S(n))$, số giả Frobenius $PF(S)$, giống $g(S(n))$ và kiểu $t(S(n))$ của nửa nhóm số Mersenne $S(n)$ (mục 2.3).

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Lương Ngọc Nhật (2017), *Một số bất biến của nửa nhóm số*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.
- [2] Nguyễn Hà Trang (2021), *Số Frobenius bình phương*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.
- [3] Hoàng Thế Toàn (2020), *Về vấn đề Frobenius cho các nửa nhóm số*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.

Tiếng Anh

- [4] J.C. Rosales, P.A. García- Sánchez (2009), *Numerical semigroups*, Development in mathematics, **20**, Springer.
- [5] J.C. Rosales, M.B. Branco and D. Torráo (2017), The Frobenius problem for Mersenne numerical semigroups, *Mathematische Zeitschrift*, **286**, 741-749.
- [6] Denise Miriam Mendes Torráo (2017), *Combinatory Problems in Numerical Semigroups*, PhD thesis in Mathematics, University of Évora.