COMPOSITES IN SEMIRINGS OF BOOLEAN GROUPS

KAMALAKSHYA MAHATAB

Abstract. We estimate the number of composite elements in the n-th grade of a group semiring of finite boolean groups. In view of this result we conjecture that the composites in these semirings of finite groups are thinly dispersed.

1. Introduction

A semiring S is a commutative monoid with an addition '+' and also a monoid with a multiplication '.' such that the multiplication is distributive over addition [3]. In this article, we will consider group semirings S with an additive identity '0' and with a multiplicative identity '1'. We will define units in a semiring S as follows:

Definition 1. *A non-zero element $u \in S$ is called a unit in S, if there exist an element $v \in S$ such that $u.v = 1$. We will denote the group of units of S as $\mathcal{U}(S)$.*

In particular $1 \in \mathcal{U}(S)$. Now we may define reducible and irreducible elements in a group semiring.

Definition 2. *We will define a non-zero non-unit element $w \in S$ as a prime, if for every $u, v \in S$ with $uv = w$, we have either u or v is a unit.*

A non-zero non-unit element of S which is not prime will be called a composite.

We will consider semirings constructed from finite groups.

Definition 3. *Let*

$$\mathbb{N} := \{0, 1, 2, \ldots\},$$

and G be a finite group. We define the group semiring $\mathbb{N}[G]$ as

$$\mathbb{N}[G] = \left\{ \sum_{g \in G} a_g g : a_g \in \mathbb{N} \right\}$$

Department of Mathematical Sciences, NTNU Trondheim, Norway

E-mail address: accessing.infinity@gmail.com, kamalakshya.mahatab@ntnu.no.

2010 *Mathematics Subject Classification.* 16Y60, 11N05, 20C05.

Key words and phrases. Semirings, Boolean groups, Multiplication table problem.

The author is supported by Grant 227768 of the Research Council of Norway, and this work was carried out when he was a research fellow at the Institute of Mathematical Sciences, Chennai.

with point-wise addition and multiplication inherited from the group G:

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g,$$
$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}\left(\sum_{\substack{g_1,g_2\\ g_1g_2=g}} a_{g_1}b_{g_2}\right) g,$$

where $a_g, b_g \in \mathbb{N}$ for all $g \in G$.

We will write $1.g$ as g, and $\sum_{g\in A} 0.g$ as 0 for any subset A of G. For a $k \in \mathbb{N}$, define the kth grade of $\mathbb{N}[G]$ as

$$\mathbb{N}[G]_k := \left\{\sum_{g\in G} a_g g \in \mathbb{N}[G] \colon \sum_{g\in G} a_g = k\right\}.$$

With the above notations, the set of units of $\mathbb{N}[G]$ is

$$\mathcal{U}\left(\mathbb{N}[G]\right) = \{g : g \in G\} = \mathbb{N}[G]_1.$$

As the augmentation map

$$\Psi_G^{(0)} : \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$$

is a semiring homomorphism, $\mathbb{N}[G]$ is graded:

$$\mathbb{N}[G]_k + \mathbb{N}[G]_l \subseteq \mathbb{N}[G]_{k+l},$$
$$\mathbb{N}[G]_k\mathbb{N}[G]_l \subseteq \mathbb{N}[G]_{kl}, \text{ for all } k, l \in \mathbb{N}.$$

The map $\Psi_G^{(0)}$ corresponds to the trivial representation of G. We will write $\mathrm{Comp}\left(\mathbb{N}[G]\right)_k$ for the set of composite elements of $\mathbb{N}[G]_k$ and $\mathrm{Pr}\left(\mathbb{N}[G]\right)_k$ for the set of primes of $\mathbb{N}[G]_k$. In this article we will attempt to give a 'good' upper bound for $|\mathrm{Comp}\left(\mathbb{N}[G]\right)_k|$. As an initial step, we make the following observations.

Theorem 1. *Let p be any prime number and let e denote the identity element in a finite group G. Then the following statements hold:*

(i) *All the elements in the p-th grade of $\mathbb{N}[G]$ are prime:*

$$\mathrm{Pr}\left(\mathbb{N}[G]\right)_p = \mathbb{N}[G]_p.$$

In particular,

$$\left|\mathrm{Pr}\left(\mathbb{N}[G]\right)_p\right| = \binom{p + |G| - 1}{p - 1}.$$

(ii) *For $n \geq 2$,*

$$\mathrm{Comp}\left(\mathbb{N}[G]\right)_n = \bigcup_{\substack{d|n,\\ 1<d<n}} \mathbb{N}[G]_d\mathbb{N}[G]_{n/d}.$$

(iii) *For $n \geq 2$ and for any $h \in G$ with $h \neq e$, the element*

$$e + (n-1)h$$

of $\mathbb{N}[G]$ is a prime.

The last statement in the above theorem says that each grade of $\mathbb{N}[G]$ has a prime in it. Also we know that $\mathbb{N}[G]_p$ has no composite elements when p is prime. We may ask:

How many composite elements are there in $\mathbb{N}[G]_n$ when n is not a prime number?

This is a difficult question to answer in general. In this article, we give some answer to this question for the case $G = (\mathbb{Z}/2\mathbb{Z})^l$. Even then, we will see that the upper bounds of $\mathrm{Comp}\left(\mathbb{N}[G]\right)_k$ requires some non-trivial results from number theory.

Before we proceed further, we would like to define some notations that we will use throughout the article.

Notations. *Let $f(x)$ be any real or complex valued function and let $g(x)$ be a real valued function which is positive for sufficiently large real numbers x. Then*

(i) *$f(x) \ll g(x)$, if there exist a real number x_0 and a positive constant C depending on x_0 such that $|f(x)| \leq Cg(x)$ for all $x \geq x_0$. If we denote $f(x) \ll_{k_1,\ldots,k_r} g(x)$, then $|f(x)| \leq Cg(x)$ for all $x \geq x_0$ and the constant C depends on the parameters $k_1, \ldots, k_r$.*

(ii) *$f(x) \gg g(x)$, if there exist a real number x_0 and a positive constant C depending on x_0 such that $|f(x)| \geq Cg(x)$ for all $x \geq x_0$. As before, $f(x) \gg_{k_1,\ldots,k_r} g(x)$ means $|f(x)| \geq Cg(x)$ for all $x \geq x_0$ and the constant C depends on the parameters $k_1, \ldots, k_r$.*

(iii) *$f(x) \asymp g(x)$, if $f(x) \ll g(x)$ and $f(x) \gg g(x)$. Similarly, $f(x) \asymp_{k_1,\ldots,k_r} g(x)$ would mean $f(x) \ll_{k_1,\ldots,k_r} g(x)$ and $f(x) \gg_{k_1,\ldots,k_r} g(x)$.*

We may observe that $|\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n| = \binom{n+2^l-1}{2^l-1} \asymp_l n^{2^l-1}$. Let

$$\Theta_l(n) := \left|\mathrm{Comp}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]\right)_n\right|.$$

By Theorem 1,

$$\begin{aligned}\Theta_l(n) &\leq |\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n - |\{g_1 + (n-1)g_2 : g_1, g_2 \in \mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l\}| \\ &\leq \binom{n+2^l-1}{2^l-1} - 2^{2l} + 2^l.\end{aligned}$$

But this is a very crude upper bound. To compute an upper bound for $\Theta_l(n)$ when n does not have too many prime factors, we need the following result of Kevin Ford.

Theorem 2 (Ford[1, 2])**.** *For $m \leq n$ and $a_1, a_2, b_1, b_2 \in \mathbb{N}$, we have*

$$|\{a_1 + jb_1 : 1 \leq j \leq m\}\{a_2 + jb_2 : 1 \leq j \leq n\}| \asymp \frac{mn}{(\log m)^\delta (\log\log m)^{3/2}},$$

where [1]

$$\delta = 1 - \frac{1 + \log\log 2}{\log 2}.$$

We will only give a sketch of the proof of Theorem 2 as it is an easy consequence of Ford's proof. In [1, 2], Ford proved that

$$|\{j_1 j_2 : 1 \leq j_1, j_2 \leq n\}| \asymp \frac{n^2}{(\log n)^\delta (\log\log n)^{3/2}}, \quad n \to \infty.$$

[1]We will fix the notation $\delta = 1 - \frac{1+\log\log 2}{\log 2}$ throughout this article.

This proof also implies

(1)
$$|\{j_1 j_2 : 1 \le j_1 \le m, j_2 \le n\}| \asymp \frac{mn}{(\log n)^{\delta}(\log\log n)^{3/2}}, \quad \text{when } m \le n,\ m \to \infty.$$

Further note that

$$\begin{aligned} &|\{(a_1 + j_1 b_1)(a_2 + j_2 b_2) : 1 \le j_1 \le m, 1 \le j_2 \le n\}| \\ &= |\{b_1 j_1 b_2 j_2 : 1 \le j_1 \le m, j_2 \le n\}| + O(m+n). \end{aligned} \tag{2}$$

So Theorem 2 follows from (1) and (2).

Using the above estimate, we prove the following theorem.

Theorem 3. *Let k be a fixed positive integer. Let $P^-(n)$ denote the smallest prime factor of n for a positive integer $n \ge 2$. Further, if n has at most k prime factors, then*

$$\Theta_l(n) \ll_{k,l} \left(\frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}}\right)^{2^l-1} \qquad as \quad P^-(n) \to \infty.$$

For $l = 1$,

$$\Theta_1(n) \asymp_k \frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}} \qquad as \quad P^-(n) \to \infty.$$

Theorem 3 suggests that for any finite group G, the number of composites is less than the number of primes in the n-th grade of the group semiring. In other words,

Conjecture 1. *Let G be a finite group and let the number of prime factors of n be bounded by k. Then*

$$\lim_{P^-(n)\to\infty} \frac{|\mathrm{Comp}\,(\mathbb{N}[G])_n|}{|\mathbb{N}[G]_n|} = 0.$$

We would like to mention that we could not find any relevant literature on the above conjecture. Similar questions can be formulated for primes in different classes of positive matrices (see [6]). A question related to this investigation has been asked by Y. Ginosar in [5]: Is there a sufficient condition on G that would make factorization of an element in $\mathbb{N}[G]$ unique? This question of Ginosar was motivated by paper of Gilmer and Parker [4] which investigates unique factorization in group ring $R[G]$, where R is an integral domain and G is an abelian group.

To prove Theorem 3, we used the fact that the representations of $(\mathbb{Z}/2\mathbb{Z})^l$ are one-dimensional and rational. In other words, $\mathbb{Q}\left[(\mathbb{Z}/2\mathbb{Z})^l\right]$ splits completely in one-dimensional representations, which allows us to rephrase our question on primes in group semirings in terms of certain distribution of prime numbers. However, this is not true for other groups, which is the main obstacle in proving Conjecture 1.

2. Proofs Of The Theorems

2.1. **Proof of Theorem 1.** Proofs of (i) and (ii) follows from the definitions. To prove (iii), let

$$\sum_{g\in G} a_g g,\ \sum_{g\in G} b_g g \ \in\ \mathbb{N}[G]$$

be such that

$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = e + (n-1)h.$$

We equate the coefficients of the above equation to have the following identities:

$$\sum_{g\in G} a_g b_{g^{-1}} = 1, \tag{3}$$

$$\sum_{g\in G} a_g b_{g^{-1}h} = n-1, \tag{4}$$

$$\sum_{g\in G} a_g b_{g^{-1}h'} = 0 \quad \text{for } h' \neq e, h. \tag{5}$$

Let for some $g_0 \in G, a_{g_0} \neq 0$ and it contributes to the sum in (3). Then

$$a_{g_0} = b_{g_0^{-1}} = 1. \tag{6}$$

Since $a_{g_0} = 1$, from (5) we get

$$b_{g_0^{-1}h'} = 0 \quad \text{for} \quad h' \neq e, h. \tag{7}$$

Now (4) and (7) will imply

$$a_{hg_0} b_{(hg_0)^{-1}h} + a_{g_0} b_{g_0^{-1}h} = n-1.$$

Since $a_{g_0}, b_{g_0^{-1}} = 1$, we have

$$a_{hg_0} + b_{g_0^{-1}h} = n-1. \tag{8}$$

If $a_{hg_0} = 0$, then $b_{g_0^{-1}h} = n-1$. This will imply $\sum_{g\in G} a_g g = g_0$, which proves (iii). So suppose $a_{hg_0} \neq 0$. We will prove (iii), if we show $b_{g_0^{-1}h} = 0$. If $h = h^{-1}$, then by (3),

$$a_{hg_0} b_{g_0^{-1}h^{-1}} = 0 \implies b_{g_0^{-1}h} = 0.$$

If $h \neq h^{-1}$, then h^2 is different from h and e. We use (5) in this case to have

$$a_{hg_0} b_{(g_0^{-1}h^{-1})h^2} = 0 \implies b_{g_0^{-1}h} = 0.$$

This proves (iii).

2.2. **Proof of Theorem 3.** We will first prove the theorem for the case $l = 1$. Let

$$\mathbb{Z}/2\mathbb{Z} = \{\alpha_0, \alpha_1\},$$

with α_0 being the identity element. Define a map Ψ as follows:

$$\begin{aligned} \Psi : \mathbb{N}[\mathbb{Z}/2\mathbb{Z}] &\longrightarrow \mathbb{Z} \\ a\alpha_0 + b\alpha_1 &\longrightarrow a - b. \end{aligned}$$

The map Ψ is a semiring homomorphism; in other words, it preserves multiplication and addition of $\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]$ in the ring $\mathbb{Z}$. Let Ψ_n be the restriction of Ψ to $\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_n$. We may also observe that Ψ_n is a one to one map. If $n = m_1 m_2$ for $m_1, m_2 > 1$, then

$$\begin{aligned} &\Psi_n\left(\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_1}\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_2}\right) = \Psi\left(\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_1}\right)\Psi\left(\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_2}\right) \\ &= \{-m_1, -(m_1-2), \ldots, m_1-2, m_1\}\{-m_2, -(m_2-2), \ldots, m_2-2, m_2\}. \end{aligned}$$

If we assume $m_1 \leq m_2$, then by Theorem 2 we have

$$|\Psi_n\left(\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_1}\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{m_2}\right)| \asymp \frac{n}{(\log m_1)^{\delta}(\log\log m_1)^{3/2}} \text{ as } \quad m_1 \to \infty. \tag{9}$$

From Theorem 1 and (9) we get

$$\begin{aligned}|\Psi_n\left(\mathrm{Comp}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})]\right)_n\right)| &= \left|\Psi_n\left(\bigcup_{\substack{d|n,\\ 1<d<n}} \mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_d\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{n/d}\right)\right| \\ &\leq 2\sum_{\substack{d|n\\ 1<d\leq\sqrt{n}}} \frac{n}{(\log d)^{\delta}(\log\log d)^{3/2}}. \\ &\ll_k \frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}}.\end{aligned}$$

Considering only $\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{P^-(n)}\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{n/P^-(n)}$, we have

$$\begin{aligned}|\Psi_n\left(\mathrm{Comp}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})]\right)_n\right)| &\geq \left|\Psi_n\left(\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{P^-(n)}\mathbb{N}[\mathbb{Z}/2\mathbb{Z}]_{n/P^-(n)}\right)\right| \\ &\gg \frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}}.\end{aligned}$$

This proves the required result for $l = 1$.

For $l > 1$, instead of Ψ we consider all the nontrivial characters of $(\mathbb{Z}/2\mathbb{Z})^l$. Denote these characters by

$$\Psi^{(1)}, \ldots, \Psi^{(2^l-1)}.$$

We can show that

$$\Psi_n^{(j)}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n\right) = \{-n, -n+2, \ldots, n-2, n\}.$$

Similar to the case $l = 1$, using Theorem 2, we can show that for $l > 1$ and $m_1 \leq m_2$,

$$\Psi_n^{(j)}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_{m_1}\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_{m_2}\right) \asymp \frac{n}{(\log m_1)^{\delta}(\log\log m_1)^{3/2}}.$$

If we know $\Psi_n^{(j)}(a)$ for $j = 1, \ldots, 2^l - 1$ and that $a \in \mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n$, then we can compute a. This gives

$$\begin{aligned}&\left|\mathrm{Comp}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n\right)\right| \leq \prod_{j=1}^{2^l-1}\left|\Psi_n^{(j)}\left(\mathrm{Comp}\left(\mathbb{N}[(\mathbb{Z}/2\mathbb{Z})^l]_n\right)\right)\right| \\ &\leq \prod_{j=1}^{2^l-1}\left(\sum_{\substack{d|n\\ 1<d\leq\sqrt{n}}} \frac{n}{(\log d)^{\delta}(\log\log d)^{3/2}}\right) \ll \prod_{j=1}^{2^l-1} 2^k \frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}} \\ &\ll_{k,l} \left(\frac{n}{(\log P^-(n))^{\delta}(\log\log P^-(n))^{3/2}}\right)^{2^l-1}.\end{aligned}$$

This completes the proof for $l > 1$.

Acknowledgement

The author would like to thank Anirban Mukhopadhyay and Amritanshu Prasad for several fruitful discussions.

References

[1] K. Ford. *The distribution of integers with a divisor in a given interval.* Ann. of Math.(2), 168, no.2 (2008), pp. 367–433.

[2] K. Ford. *Integers with a divisor in* $(y, 2y]$. Anatomy of integers, CRM Proc. Lecture Notes, 46 (2008), Amer. Math. Soc., Providence, RI, pp. 65–80.

[3] J. S. Golan. *Semirings and their applications.* Kluwer Academic Publishers, Dordrecht, (1999).

[4] R. Gilmer – T. Parker. *Divisibility properties in semigroup rings.* Michigan Math. J., 21 (1974), pp. 65–86.

[5] Y. Ginosar. *ADV–1I, ADV Perspectives in Group Theory.* Adv. Group Theory Appl., 1(2016), pp. 156–157.

[6] G. Picci – J. M. van den Hof – J. H. van Schuppen. *Primes in several classes of the positive matrices.* Linear Algebra Appl., 277, no. 1–3(1998), pp. 149–185.