具圓性平面近環之重疊問題

計畫類別：個別型計畫
計畫編號：
執行期間：
執行單位：國立成功大學數學系暨應用數學所

計畫主持人：柯文峰

報告類型：完整報告
處理方式：本計畫可公開查詢

中華民國 92 年 10 月 31 日
1. Introduction

First there were planar nearrings. The first three examples of them were found by twisting the multiplication of the complex number field (Clay [1]). Two of them were used as models for many researches in the following twenty years. Especially, the connection of planar nearrings and geometry and combinatorial structures were established. The remaining one puzzled researchers for many years till 1988 when Clay [2] introduced the notion of circularity for planar nearrings. This third example of planar nearring build on the complex number field $\mathbb{C}$ was the one with a new multiplication defined by

$$a \ast b = \begin{cases} 0, & \text{if } a = 0; \\ (a/|a|)b, & \text{if } a \neq 0, \end{cases}$$

for all $a, b \in \mathbb{C}$. The natural incidence structure obtained from this planar nearring is $(\mathbb{C}, \mathscr{B}_T^*, \in)$, where $T$ is the unit circle and $\mathscr{B}_T^*$ is the set of all circles in the complex plane.

In an attempt to understand more of the circularity property of circular planar nearrings, Clay took again the planar nearring $(\mathbb{C}, +, \ast)$ and introduced an equivalence relation on the set of circles $\mathscr{B}_T^*$. A typical equivalence class under this relation is $E_{rc} = \{Tr + b \mid b \in Tc\}$, where $r$ and $c$ are nonzero complex numbers. Each $E_{rc}$ is the family of circles with radius $r$ and centers on the circle $Tc$. Then a graph is assigned to each $E_{rc}$ in order to understand the behavior of $E_{rc}$ (cf. [3, §6]). This idea has provided fruitful results since. In particular, applications to coding theory providing optimal codes and cryptography earn circular planar nearrings good reputations as applicable algebraic structures.

In [7], we studied these $E_{rc}$'s for circular planar nearrings constructed from a ring using a cyclic subgroup of order $k$ of the unit group. It turns out that each graph of an $E_{rc}$ can be decomposed into a union of some basic graphs. These graphs give circular planar nearring some symmetric appearances, which is unusual in the highly nonsymmetric nearring structure (due to the lacking of one side distributive law). Moreover, for a fixed non zero $r$, the total number of basic graphs occurring in the graphs of $E_{rc}$'s, $c \in \mathbb{C}^*$, depends on $k$ alone. This study leads to our description of the solutions of the equation $x^n + y^n - z^n = 1$ in finite fields. See [6].

A basic question that one can ask about these graphs is whether one can give a formula of counting as a function of $k$, say. Such a question may not be easy, or even possible to answer. However, a first step to take tackling this question would be to understanding when two basic graphs will overlap each other. We have noticed an phenomenon for field generated planar nearrings that some basic graphs always occur together as subgraphs of certain $E_{rc}$'s regardless of the underlying field.
In this project, we have tried the first attempt towards this problem. Namely, we studied the following. Let $k \geq 3$. Let $\Phi$ be the subgroup of order $k$ in the multiplicative group $\mathbb{C}^*$. For a fixed $r \in F \setminus \{0\}$, define $E_r^c = \{\Phi r + b \mid b \in \Phi c\}$. Let $G(E_r^c)$ be the graph with vertices $\Phi c$, and two vertices $c_1, c_2 \in \Phi c$ is connected by an even or odd edge according to $(\Phi r + c_1) \cap (\Phi r + c_2)$ contains 1 or 2 elements, otherwise, there is no edges connecting $c_1$ and $c_2$. If a graph $G(E_r^c)$ is non-null (some vertices are connected by an edge), then either it is a basic graph or it is a union of spanning subgraphs (see [7]). We fully understand when a graph $G(E_r^c)$ is a union of spanning subgraphs. Explicitly, we describe the solutions that lead to nontrivial overlaps of basic graphs appearing in the set of graphs $\{G(E_r^c) \mid c \in \mathbb{C}^*\}$.

2. The settings

Let $k \geq 3$ be a fixed integer. We denote $\varphi = \exp(2\pi i/k)$ for a primitive $k$th root of unity in $\mathbb{C}$, and let $\Phi = \langle \varphi \rangle$ be the subgroup of order $k$ of the group of units in $\mathbb{C}^*$. We fix a nonzero $r \in \mathbb{C}^*$. Then a graph $G(E_r^c)$, $c \in \mathbb{C}^*$, has a non-null edge if and only if $\Phi r + c \cap \Phi r + \varphi^i(c) \neq \emptyset$ for some $i \in \{1, 2, \ldots, k-1\}$, and $G(E_r^c)$ contains two (distinct) basic graphs means that there are two distinct $s, t, u, v \in \{1, 2, \ldots, k-1\}$ with $s + u \neq k$ such that $\Phi r + c \cap \Phi r + \varphi^s(c) \neq \emptyset$ and $\Phi r + c \cap \Phi r + \varphi^u(c) \neq \emptyset$. This last situation is equivalent to that there are $s, t, u, v, i, j \in \{1, 2, \ldots, k-1\}$ such that $s + u \neq k$ and

$$\varphi^i(\varphi^i - 1)(r) = (\varphi^s - 1)(c) \quad \text{and} \quad \varphi^j(\varphi^v - 1)(r) = (\varphi^u - 1)(c).$$

Dividing the second equality into the first, we see that two distinct basic graphs appear at the same time in the graph $G(E_r^c)$ if and only if

$$\varphi^\omega \varphi^t - 1 = \varphi^u - 1, \quad \varphi^s - 1,$$

where $s, t, u, v \in \{1, \ldots, k/2-1\}$ and $\omega \in \mathbb{Z}$. Here we may assume that $v+s \geq u+t$.

Now, expanding the equation, we see that two distinct basic graphs appear at the same time in the graph $G(E_r^c)$ if and only if

$$\varphi^{u+s} - \varphi^u - \varphi^s + 1 - \varphi^{\omega u+t} + \varphi^{\omega u} + \varphi^{\omega+t} - \varphi^\omega = 0$$

for some $s, t, u, v \in \{1, \ldots, k/2-1\}$ and $\omega \in \mathbb{Z}$. We note that this last equation represents a vanishing sum involving 8 terms except in the trivial cases that $v = u$ (hence $s = t$ and $\omega = 0$) or $u = s$ (hence $v = t$ and $\omega = 0$), and we shall refer to these solutions as trivial solutions. These solutions correspond to the overlaps in $G(E_r^c)$. The following theorem of Conway and Johns now comes in handy.

*Theorem 2.1 ([4, Theorem 6]).* Let $S$ be a nonempty vanishing sum of length at most 9. Then either $S$ involves $\theta, \alpha \theta, \alpha^2 \theta$ for some root $\theta$, or $S$ is similar to one of

\[
\begin{align*}
1 + \beta + \beta^2 + \beta^3 + \beta^4, & \quad -\alpha - \alpha^2 + \beta + \beta^2 + \beta^3 + \beta^4, \\
1 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \gamma^6, & \quad 1 + \beta + \beta^4 - (\alpha + \alpha^2)(\beta^2 + \beta^3), \\
-\alpha - \alpha^2 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \gamma^6, & \quad \beta + \beta^4 - (\alpha + \alpha^2)(1 + \beta + \beta^2), \\
1 + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 - (\alpha + \alpha^2)(\gamma + \gamma^6), & \quad 1 - (\alpha + \alpha^2)(\beta + \beta^2 + \beta^3 + \beta^4),
\end{align*}
\]

where $\alpha, \beta, \gamma$ are primitive roots of orders 3, 5, 7 respectively.
Applying this theorem, we see that, except for the trivial cases, the vanishing sum (2.2) takes one of the following forms

\begin{align}
(2.3) & \quad \lambda_1(1 + \alpha + \alpha^2) + \lambda_2(1 + \alpha + \alpha^2) + \lambda_3(1 - 1), \\
(2.4) & \quad \lambda_1(-\alpha - \alpha^2 + \beta + \beta^2 + \beta^3 + \beta^4) + \lambda_2(1 - 1), \\
(2.5) & \quad \lambda_1(1 + \alpha + \alpha^2) + \lambda_2(1 + \beta + \beta^2 + \beta^3 + \beta^4), \\
(2.6) & \quad \lambda(\beta + \beta^4 - (\alpha + \alpha^2)(1 + \beta^2 + \beta^3)), \\
(2.7) & \quad \lambda(-\alpha - \alpha^2 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \gamma^6),
\end{align}

3. The results

Our first result is that Φ has even order when there are nontrivial overlaps other than those appear in \(G(E_r^2)\). Also, as the third root of unity \(\alpha\) and \(\alpha^2\) are part of the terms in every case, we see that Φ actually contains \(\alpha\).

**Theorem 3.1.** If (2.2) has nontrivial solutions, then \(-1, \alpha \in \Phi\). Consequently, the order of Φ is divisible by 6.

Next, since the principle argument of \(\varphi^{r-1}/\varphi^{s-1}\) is \((t - s)\pi/2k\) while that of \(\varphi^{t-1}/\varphi^{s-1}\) is \((v - u)\pi/2k\), we have \(\varphi = \exp((v - u - (t - s))\pi i/2k)\), and so

\[\omega = k + (v + s - (u + t))/2.\]

Using this relation, we can rewrite (2.2) as

\[
\varphi^{k/2 + (v+s+u-t)/2} + \varphi^{k/2 + (v+s-u+t)/2} + \varphi^{(v+s+u+t)/2} + \varphi^{(v+s-u-t)/2} + \varphi^v + \varphi^s + \varphi^{k/2 + (v+s)} + \varphi^{k/2} = 0. \tag{3.1}
\]

Here, we recall that \(\varphi^{k/2} = -1\).

Finally, we have the following solutions.

**Theorem 3.2.** If (3.1) takes the form

\[\lambda_1(1 + \alpha + \alpha^2) + \lambda_2(1 + \alpha + \alpha^2) + \lambda_3(1 - 1),\]

then one of the following holds:

1. \(u = t\), and \(\{s, v\} = \{5k/12, k/12\}\);
2. \(s = v\) or \(s - v = k\) or \(v - s = k\);
3. \(u = t = k/6\).

**Theorem 3.3.** If (3.1) takes the form

\[\lambda_1(-\alpha - \alpha^2 + \beta + \beta^2 + \beta^3 + \beta^4) + \lambda_2(1 - 1),\]

then one of the following holds:

1. \(\{v, s\} = \{5k/12, k/12\}\), \(u = 3k/10\) and \(t = k/10\);
2. \(u = 4k/15\), \(t = k/15\), and \(\{v, s\} = \{k/20, 9k/20\}\);
3. \(\{v, s\} = \{3k/20, 7k/20\}\), \(u = 7k/15\) and \(t = 2k/15\).

**Theorem 3.4.** If (3.1) takes the form

\[\lambda_1(1 + \alpha + \alpha^2) + \lambda_2(1 + \beta + \beta^2 + \beta^3 + \beta^4),\]

then one of the following holds:

1. \(u = t = 3k/10\), and \(\{v, s\} = \{7k/30, 13k/30\}\);
2. \(v = s = k/6\), \(u = 3k/10\) and \(t = k/10\);
3. \(v = 11k/30\), \(s = k/30\), and \(u = t = k/10\).
Theorem 3.5. If (3.1) takes the form
\[ \lambda(-\alpha - \alpha^2 + \gamma + \gamma^2 + \gamma^3 + \gamma^4 + \gamma^5 + \gamma^6), \]
then one of the following holds:

1. \[ u = 3k/14, \quad t = k/14, \quad \{v, s\} = \{10k/21, 4k/21\}; \]
2. \[ u = 5k/14, \quad t = k/14, \quad \{v, s\} = \{2k/21, 5k/21\}; \]
3. \[ u = 3k/14, \quad t = k/14, \quad \{v, s\} = \{8k/21, k/21\}; \]
4. \[ u = 5k/14, \quad t = 3k/14, \quad \{v, s\} = \{4k/21, 10k/21\}. \]

4. Conclusions

Although we have now fully understood the overlaps in the complex plane case, there is still a long way to go for uncovering the general situation. Our next step would be to work on the finite fields situation. This is because that the graphs in finite fields situation behave like that of complex plane case when the characteristic is large enough [8]. On the other hand, the study of the graphs produced from nonabelian \( \Phi \) also provides another possible direction to explore the overlap [5] phenomenon.

References