Primjer 3.3 (Paleyevi grafovi). Neka je $q \equiv 1 \pmod{4}$ potencija prostog broja. Za skup vrhova uzmemo elemente konačnog polja $\mathbb{F}_q$. Vrhovi x i y su susjedni ako je $x - y$ kvadrat u $\mathbb{F}_q \backslash \{0\}$. Tako dobijemo jako regularan graf s parametrima $SRG\left(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1)\right)$.

Zadatak 3.4. Dokažite da konstrukcija iz primjera 3.3 zaista daje jako regularne grafove.

Rješenje.

1. dio: Pokazati da je relacija susjedstva $x \sim y \iff x - y \in (\mathbb{F}_q^*)^2$ simetrična.

Dokaz.

Kako je $x - y = -1(y - x)$, dovoljno je pokazati da je $-1 \in (\mathbb{F}_q^*)^2$. Budući da je $q \equiv 1 \pmod 4$, slijedi da $4 | q - 1$.

Označimo sa a primitivni element cikličke grupe $\mathbb{F}_q^*$.

Tada vrijedi da je $q-1$ najmanji prirodan broj takav da je $a^{q-1}=1$, što možemo zapisati kao $a^{q-1}-1=\left(a^{\frac{q-1}{2}}-1\right)\left(a^{\frac{q-1}{2}}+1\right)=0$.

Kako je $\left(a^{\frac{q-1}{2}}\right)\neq 1$, slijedi da je $a^{\frac{q-1}{2}}=\left(a^{\frac{q-1}{4}}\right)^2=-1$.

Iz toga slijedi da je $a^{\frac{q-1}{4}}$ kvadratni korijen od -1, tj. da je $-1\in(\mathbb{F}_q^*)^2$.

Dakle, relacija $\sim$ je simetrična.

2. dio: Pokazati da je Paleyev graf jako regularan s paramterima $SRG\left(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1)\right)$.

Dokaz.

i) $k = \frac{1}{2}(q-1)$.

Budući da je a primitivni element (generator multiplikativne grupe) $\mathbb{F}_q^*$, vrijedi da su parne potencije od a kvadrati, a neparne su nekvadrati. Kako je broj vrhova grafa jednak q, onda je svaki vrh susjedan s ukupno $\frac{q-1}{2}$ vrhova.

Asocijacijske sheme

Zadatak 3.4

ii) $\lambda = \frac{1}{4}(q-5)$.

Za vrhove x i y treba odrediti kardinalitet skupa $\{\, z \mid x-z,\ z-y \in (\mathbb{F}_q^*)^2 \,\}$. Ako promotrimo skup $\{\, z \mid (x-z)(z-y) \in (\mathbb{F}_q^*)^2 \,\}$, uz oznake $X = N(x)$ i $Y = N(y)$, tada je $Z = (X \cap Y) \cup (X^c \cap Y^c)$.

Za skup Z vrijedi:

$$\begin{aligned} |Z| &= |(X \cap Y) \cup (X^c \cap Y^c)| \\ &= |X \cap Y| + |X^c \cap Y^c| \\ &= |X \cap Y| + q - |X \cup Y| \\ &= |X \cap Y| - |X| - |Y| + |X \cap Y| \\ &= 2|X \cap Y| + q - 2 \cdot \frac{q-1}{2} \\ &= 2|X \cap Y| + 1. \end{aligned} \tag{1}$$

Cilj je pokazati da je $|Z| = \begin{cases} \dfrac{q-3}{2}, & \text{ako } x \sim y, \\ \dfrac{q-1}{2}, & \text{ako } x \not\sim y. \end{cases}$

Tada, budući da je $|X \cap Y| = \lambda$ ako je $x \sim y$ te da je $|X \cap Y| = \mu$ ako je $x \not\sim y$, lako dolazimo do traženog rezultata za parametre λ i μ. Dakle, razlikujemo dva slučaja.

Definiriamo funkciju $\chi(x) = \begin{cases} 1, & \text{ako } x \in (\mathbb{F}_q^*)^2, \\ -1, & \text{ako } x \notin (\mathbb{F}_q^*)^2. \end{cases}$

Napomena. Funkciju χ nazivamo kvadratni karakter modulo q.

Prvi slučaj; $x \sim y$, $x, y \notin Z$.

$$|Z| = \sum_{z \notin \{x,y\}} \frac{1}{2}(1 + \chi((x-z)(y-z))) = \frac{q-2}{2} + \frac{1}{2} \sum_{z \notin \{x,y\}} \chi((x-z)(y-z)). \quad (2)$$

Napomena. Ovdje se koristi rezultat da je umnožak dvaju nekvadrata kvadrat u konačnom polju $\mathbb{F}_q^*$.

Sumu možemo zapisati u obliku

$$\sum_{z \notin \{x,y\}} \chi\left(\frac{x-z}{y-z}\right),$$

koristeći pritom da za $z \neq y$ vrijedi $\chi(y-z) = \chi\left(\frac{1}{y-z}\right)$.

Napomena. $y - z$ je kvadrat $\iff$ $\frac{1}{y-z}$ je kvadrat.

Dakle,

$$\sum_{z\notin\{x,y\}} \chi((x-z)(y-z)) = \sum_{z\notin\{x,y\}} \chi\left(\frac{x-z}{y-z}\right) = \sum_{z\notin\{x,y\}} \chi\left(1+\frac{x-y}{y-z}\right).$$

Označimo sa $w := \frac{x-z}{y-z}$. Tada je $z = y - \frac{x-y}{w-1}$. Ako je $z \notin \{x,y\}$, onda je $1+\frac{x-y}{y-z} \notin \{0,1\}$.

(Ako $x \neq z$, onda je $\frac{x-y}{y-z} \neq -1$ i $x \neq y$, pa je $\frac{x-y}{y-z} \neq 0$).

Budući da su točno pola nenul elemenata kvadrati i da iz sume izostavljamo 1, dobivamo

$$\sum_{w\notin\{0,1\}} \chi(w) = -1. \tag{3}$$

Uvrštavanjem (3) u (2) dobivamo traženi rezultat u slučaju kada je $x \sim y$:

$$|Z| = \frac{q-2}{2} + \frac{1}{2} \cdot (-1) = \frac{q-3}{2}.$$

Na kraju, izjednačavanjem posljednje jednakosti sa (1) dobivamo glavnu tvrdnju:

$$\begin{aligned} \frac{q-3}{2} &= 2|X \cap Y| + 1 \\ \frac{q-3}{2} &= 2\lambda + 1 \\ \lambda &= \frac{q-5}{4}. \end{aligned}$$

iii) $\mu = \dfrac{q-1}{4}$.

Drugi slučaj; $x \not\sim y$, $\{x,y\} \in Z$.

Slično kao u prvom dijelu, koristeći (3) zapišemo $|Z|$ u obliku

$$
\begin{aligned}
|Z| &= 2 + \sum_{z \notin \{x,y\}} \frac{1}{2}(1 + \chi((x-z)(y-z))) \\
&= 2 + \frac{1}{2} \cdot (q-2) + \frac{1}{2} \sum_{z \notin \{x,y\}} \chi((x-z)(y-z)) \\
&= q + \frac{q-2}{2} + \frac{1}{2} \cdot (-1) \\
&= \frac{q+1}{2}.
\end{aligned}
$$

Izjednačavanjem posljednje jednakosti sa (1) dobivamo glavnu tvrdnju:

$$\begin{aligned} \frac{q+1}{2} &= 2|X \cap Y| + 1 \\ \frac{q-3}{2} &= 2\mu + 1 \\ \mu &= \frac{q-1}{4}. \end{aligned}$$