Wilson's bijection and upper bounds on cyclotomic numbers

Akihiro Munemasa[1]

[1]Graduate School of Information Sciences
Tohoku University
joint work with Koichi Betsumiya, Takao Komatsu (Hirosaki Univ.)
and Mitsugu Hirasaka (Pusan National Univ.)

arXiv:1109.6539
November 19, 2011
Nagoya University

Notation

- q: a prime power, $F = \mathbb{F}_q = \mathrm{GF}(q)$.
- $F^\times = F \setminus \{0\} = \langle \alpha \rangle$.
- $e, k \in \mathbb{Z}$, $e, k \geq 2$, $ek = q - 1$.
- $C_i = \langle \alpha^e \rangle \alpha^i \quad (i = 0, 1, \ldots, e-1)$.

Then

$$C_0 = \{x^e \mid x \in F^\times\} = \{y \in F \mid y^k = 1\}.$$

$$F^\times = \bigcup_{i=0}^{e-1} C_i.$$

Example: $q = 7$, $e = 2$.

- $F^\times = \{1, 2, 3, 4, 5, 6\} = C_0 \cup C_1$.
- $C_0 = \{1, 2, 4\}$, $C_1 = \{3, 5, 6\}$.

Example: $q = 7$, $e = 2$

- $F^\times = \{1, 2, 3, 4, 5, 6\} = C_0 \cup C_1$.
- $C_0 = \{1, 2, 4\}$, $C_1 = \{3, 5, 6\}$.

C_0 is a $(7, 3, 1)$-difference set.

$$\begin{aligned} C_0 - C_0 &= \{x - y \mid x, y \in C_0\} \\ &= \{0, 0, 0, 1, 2, 3, 4, 5, 6\}. \end{aligned}$$

$x - y = 1 \iff y + 1 = x$.

$$|(C_0 + 1) \cap C_0| = 1.$$

Definition

- $F = \mathbb{F}_q = \mathrm{GF}(q)$, $F^\times = F \setminus \{0\} = \langle \alpha \rangle$.
- $e, k \in \mathbb{Z}$, $e, k \geq 2$, $ek = q - 1$.
- $C_i = \langle \alpha^e \rangle \alpha^i \quad (i = 0, 1, \dots, e-1)$.
- $F^\times = \bigcup_{i=0}^{e-1} C_i$.

Cyclotomic numbers are:

$$(i, j) = |(C_i + 1) \cap C_j| \qquad (i, j \in \{0, 1, \dots, e-1\}).$$

Clearly $(i, j) \leq |C_j| = k$.
Their average is:

$$\frac{1}{e^2} \sum_{i,j=0}^{e-1} (i, j) = \frac{1}{e^2} |(\bigcup_{i=0}^{e-1} C_i + 1) \cap (\bigcup_{j=0}^{e-1} C_j)|$$
$$= \frac{1}{e^2} |(F^\times + 1) \cap F^\times| = \frac{q-2}{e^2} = \frac{k}{e} - \frac{1}{e^2}.$$

$C_0 = \{x \in F \mid x^k = 1\} = \{\alpha^{ej} \mid 0 \le j < k\}$

C_0 is the set of eigenvalues of the $k \times k$ matrix

$$T = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}.$$

$$(T+I)^k - I \text{ has eigenvalues } (x+1)^k - 1 \quad (x \in C_0).$$

Since $(x+1)^k - 1 = 0 \iff x + 1 \in C_0$,

$$\text{the cyclotomic number } (0,0) = |(C_0 + 1) \cap C_0|$$

counts the multiplicity of 0 as an eigenvalue of $(T+I)^k - I$, i.e.,

$$(0,0) = k - \operatorname{rank}((T+I)^k - I).$$

$(0,0) = k - \operatorname{rank}((T+I)^k - I)$. Assume $k = 2m$.

$$T = \begin{bmatrix} & 1 & & \\ & & \ddots & \\ & & & 1 \\ 1 & & & \end{bmatrix}, \quad (T+I)^k - I = \sum_{i=0}^{2m-1} \binom{2m}{i} T^i$$

$$= \begin{bmatrix} \binom{2m}{0} & \cdots & \cdots & {\color{red}\binom{2m}{m}} & \cdots & {\color{red}\binom{2m}{2m-1}} \\ \binom{2m}{2m-1} & \ddots & & \vdots & \ddots & \vdots \\ \vdots & \ddots & \binom{2m}{0} & {\color{red}\binom{2m}{1}} & \cdots & {\color{red}\binom{2m}{m}} \\ & & & \binom{2m}{0} & & \vdots \\ & & & & \ddots & \vdots \end{bmatrix}$$

Krattenthaler (1999)

$$\det \begin{bmatrix} \binom{2m}{m} & \cdots & \binom{2m}{2m-1} \\ \vdots & \ddots & \vdots \\ \binom{2m}{1} & \cdots & \binom{2m}{m} \end{bmatrix} = \prod_{i=0}^{m-1} \frac{i!(2m+i)!}{((m+i)!)^2}.$$

If q is a power of a large prime p, then $\det \neq 0$, so $\mathrm{rank}((T+I)^k - I) \geq \frac{k}{2}$, so $(0,0) \leq \frac{k}{2}$.

Theorem (Betsumiya–Hirasaka–Komatsu–M.)

Suppose that q is a power of a prime p.

1. $(0,0) \leq \lceil \frac{k}{2} \rceil - 1$ if $p > \frac{3k}{2}$.
2. $(i,j) \leq \lceil \frac{k}{2} \rceil$ if $p > \frac{3k}{2} - 1$.

Wilson's bijection

average:

$$\frac{1}{e^2}\sum_{i,j=0}^{e-1}(i,j)=\frac{k}{e}-\frac{1}{e^2}.$$

variance:

$$\frac{1}{e^2}\sum_{i,j=0}^{e-1}\left((i,j)-(\frac{k}{e}-\frac{1}{e^2})\right)^2=\frac{1}{e^2}((k-1)(k-2)+q-2-\frac{(q-2)^2}{e^2}).$$

$$\{(x,y)\in(F\setminus\{0,1\})^2 \mid \frac{x}{y},\frac{x-1}{y-1}\in C_0,\ x\neq y\}$$
$$\to\{(u,v)\in(C_0\setminus\{1\})^2 \mid u\neq v\}$$

bijective.

$$
\begin{aligned}
&(k-1)(k-2) \\
&= |\{(u,v) \in (C_0 \setminus \{1\})^2 \mid u \neq v\}| \\
&\overset{\text{Wilson}}{=} |\{(x,y) \in (F \setminus \{0,1\})^2 \mid \frac{x}{y}, \frac{x-1}{y-1} \in C_0,\ x \neq y\}| \\
&= |\{(x,y) \in (F \setminus \{0,1\})^2 \mid \frac{x}{y}, \frac{x-1}{y-1} \in C_0\}| - (q-2) \\
&= |\{(x,y) \in (F \setminus \{0,1\})^2 \mid \begin{array}{l} \exists i,\ x-1, y-1 \in C_i, \\ \exists j,\ x,y \in C_j \end{array} \}| - (q-2) \\
&= \left| \bigcup_{i,j=0}^{e-1} ((C_i+1) \cap C_j)^2 \right| - (q-2) \\
&= \sum_{i,j=0}^{e-1} (i,j)^2 - (q-2).
\end{aligned}
$$

Asymptotic behavior

average:

$$\frac{1}{e^2}\sum_{i,j=0}^{e-1}(i,j)=\frac{k}{e}-\frac{1}{e^2}.$$

variance:

$$\frac{1}{e^2}\sum_{i,j=0}^{e-1}\left((i,j)-(\frac{k}{e}-\frac{1}{e^2})\right)^2=\frac{1}{e^2}((k-1)(k-2)+q-2-\frac{(q-2)^2}{e^2}).$$

These imply

$$(i,j)=\frac{k}{e}+O(\sqrt{k})$$

if e is fixed and $k\to\infty$.

No conclusion if k is fixed and $e\to\infty$, while our result shows

$$(i,j)\le\left\lceil\frac{k}{2}\right\rceil.$$