Semi-Rational Groups

David Chillag and Silvio Dolfi

Groups Ischia 2010

April 2010
Dedicated to the memory of Silvia Lucido

- G a finite group. $Class(G)$ the set of conjugacy classes of G.

- G a finite group. $Class(G)$ the set of conjugacy classes of G.
- **Conjecture**: If $|C| \neq |D|$ for all $C \neq D \in Class(G)$ then $G \cong S_3$.

- G a finite group. $Class(G)$ the set of conjugacy classes of G.
- **Conjecture**: If $|C| \neq |D|$ for all $C \neq D \in Class(G)$ then $G \cong S_3$.
- Proved for solvable groups by Zhang (1994), and independently by Knörr,Lempken and Thielke (1995).

- G a finite group. $Class(G)$ the set of conjugacy classes of G.
- **Conjecture**: If $|C| \neq |D|$ for all $C \neq D \in Class(G)$ then $G \cong S_3$.
- Proved for solvable groups by Zhang (1994), and independently by Knörr,Lempken and Thielke (1995).
- Assume $|C| \neq |D|$ for all $C \neq D \in Class(G)$. Let $x \in G$ and m with $(m, o(x)) = 1$. Then $C_G(x) = C_G(x^m)$ so $|cl_G(x)| = |cl_G(x^m)|$. So x and x^m must be conjugate.

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

- Equivalnet to $x \in G$ is **rational** are:

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

- Equivalnet to $x \in G$ is **rational** are:

1. $\left| \frac{N_G(<x>)}{C_G(x)} \right| = \phi(|x|)$, ϕ Euler function.

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

- Equivalnet to $x \in G$ is **rational** are:

1. $\left| \frac{N_G(<x>)}{C_G(x)} \right| = \phi(|x|)$, ϕ Euler function.
2. $\chi(x)$ is rational (integer) for all $\chi \in Irr(G)$.

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

- Equivalnet to $x \in G$ is **rational** are:

1. $\left| \frac{N_G(<x>)}{C_G(x)} \right| = \phi(|x|)$, ϕ Euler function.
2. $\chi(x)$ is rational (integer) for all $\chi \in Irr(G)$.

Example

$G = S_n$ is rational, as x has the same cycle structure as x^m for $(m, o(x)) = 1$.

Definition

$x \in G$ is called **rational** if x is conjugate to all generators of $\langle x \rangle$. G is rational if all $x \in G$ are rational.

- Equivalnet to $x \in G$ is **rational** are:

1. $\left|\frac{N_G(<x>)}{C_G(x)}\right| = \phi(|x|)$, ϕ Euler function.
2. $\chi(x)$ is rational (integer) for all $\chi \in Irr(G)$.

Example

$G = S_n$ is rational, as x has the same cycle structure as x^m for $(m, o(x)) = 1$.

- So no restriction on $\pi(G)$, the set of prime divisors of $|G|$.

- However,

- However,

Theorem

Let G a finite rational solvable group. Then

- However,

Theorem

Let G a finite rational solvable group. Then

1. *(Gow 1976). $\pi(G) \subset \{2, 3, 5\}$.*

- However,

Theorem

Let G a finite rational solvable group. Then

1. *(Gow 1976).* $\pi(G) \subset \{2, 3, 5\}$.
2. *(Hegedűs 2005). Sylow* 5*-subgroup is normal & elementary abelian. Structure of G if* $\pi(G) = \{2, 5\}$.

- Conjecture-analog for of odd order:
ASSUMPTION: Let $|G|$ be odd such that
$|C| = |D| \Leftrightarrow C = D$ or $C = D^{-1}$,
$\forall C, D \in Class(G)$ $(D^{-1} = \{x^{-1} | x \in D\}$) .

- Conjecture-analog for of odd order:
  ASSUMPTION: Let $|G|$ be odd such that $|C| = |D| \Leftrightarrow C = D$ or $C = D^{-1}$, $\forall C, D \in Class(G)$ $(D^{-1} = \{x^{-1} | x \in D\}$) .

Theorem

(Herzog & Schönheim 2006) **ASSUMPTION** $\Leftrightarrow$ *G is nonabelian of order* 21.

- Conjecture-analog for of odd order:
ASSUMPTION: Let $|G|$ be odd such that
$|C| = |D| \Leftrightarrow C = D$ or $C = D^{-1}$,
$\forall C, D \in Class(G)$ $(D^{-1} = \{x^{-1} | x \in D\}$) .

Theorem

(Herzog & Schönheim 2006) **ASSUMPTION** $\Leftrightarrow$ *G is nonabelian of order* 21*.*

- All elements of such G are inverse semi-rational, i.e.:

- Conjecture-analog for of odd order:
  ASSUMPTION: Let $|G|$ be odd such that $|C| = |D| \Leftrightarrow C = D$ or $C = D^{-1}$, $\forall C, D \in Class(G)$ $(D^{-1} = \{x^{-1} | x \in D\})$.

Theorem

(Herzog & Schönheim 2006) **ASSUMPTION** $\Leftrightarrow$ *G is nonabelian of order 21.*

- All elements of such G are inverse semi-rational, i.e.:

Definition

$x \in G$ is inverse-semirational if every generator of $\langle x \rangle$ is conjugate to either x or x^{-1}. G itself is inverse semi-rational if all elements of G are inverse semi-rational.

- Description of odd order semi-rational groups.

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

1. *G is a Frobenius group of order $3 \cdot 7^a$.*

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

1. *G is a Frobenius group of order $3 \cdot 7^a$.*
2. *$|G| = 7 \cdot 3^a$ with a normal Frobenius subgroup of index 3.*

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

1. *G is a Frobenius group of order $3 \cdot 7^a$.*
2. *$|G| = 7 \cdot 3^a$ with a normal Frobenius subgroup of index 3.*
3. *G is a 3 - group.*

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

1. *G is a Frobenius group of order $3 \cdot 7^a$.*
2. *$|G| = 7 \cdot 3^a$ with a normal Frobenius subgroup of index 3.*
3. *G is a 3 - group.*

- All cases occur. $\exists$ inverse semi-rational 3 - groups with any exponent and derived length

- Description of odd order semi-rational groups.

Theorem

(C&D 2010) Let G be an odd order inverse semi-rational group. Then one of the followin holds:

1. *G is a Frobenius group of order $3 \cdot 7^a$.*
2. *$|G| = 7 \cdot 3^a$ with a normal Frobenius subgroup of index 3.*
3. *G is a 3 - group.*

- All cases occur. $\exists$ inverse semi-rational 3 - groups with any exponent and derived length
- The notion of inverse – semirational makes sense for even order groups as well. Is a Gow's like theorem exists ? That is: is $\pi(G)$ restricted?

- A supersolvable semi-rational group would serve as test case.

- A supersolvable semi-rational group would serve as test case.

Definition

We call $x \in G$ semi-rational if the set of generators of $\langle x \rangle$ is contained in a union of two conjugacy classes.

- A supersolvable semi-rational group would serve as test case.

Definition

We call $x \in G$ semi-rational if the set of generators of $\langle x \rangle$ is contained in a union of two conjugacy classes.

- A Frobenius group of order $6 \cdot 13$ is semi-rational but not inverse semi-rational.

- A supersolvable semi-rational group would serve as test case.

Definition

We call $x \in G$ semi-rational if the set of generators of $\langle x \rangle$ is contained in a union of two conjugacy classes.

- A Frobenius group of order $6 \cdot 13$ is semi-rational but not inverse semi-rational.

Theorem

(C&D 2010). Let G be a finite semi-rational supersolvable group (G' nilpotent suffices). Then $\pi(G) \subset \{2, 3, 5, 7, 13\}$.

- Each prime $p \in \{2, 3, 5, 7, 13\}$ divides the order of a semi-rational supersolvable group. E.g.: Frobenius group of order $\frac{1}{2}p\,(p-1)$.

- Each prime $p \in \{2, 3, 5, 7, 13\}$ divides the order of a semi-rational supersolvable group. E.g.: Frobenius group of order $\frac{1}{2}p\,(p-1)$.
- Main result:

- Each prime $p \in \{2, 3, 5, 7, 13\}$ divides the order of a semi-rational supersolvable group. E.g.: Frobenius group of order $\frac{1}{2}p\,(p-1)$.
- Main result:

Theorem

(C&D 2010). Let G be a finite semi-rational solvable group Then $\pi(G) \subset \{2, 3, 5, 7, 13, 17\}$. Furthermore, if G is inverse semi-rational then $17 \notin \pi(G)$.

- Each prime $p \in \{2, 3, 5, 7, 13\}$ divides the order of a semi-rational supersolvable group. E.g.: Frobenius group of order $\frac{1}{2}p\,(p-1)$.
- Main result:

Theorem

(C&D 2010). Let G be a finite semi-rational solvable group Then $\pi(G) \subset \{2, 3, 5, 7, 13, 17\}$. Furthermore, if G is inverse semi-rational then $17 \notin \pi(G)$.

- We do not have an example of a semi-rational solvable G with $17 \in \pi(G)$.

- GENERAL PROPERTIES

- GENERAL PROPERTIES
- The following are equivalent:

- GENERAL PROPERTIES
- The following are equivalent:

1. $x \in G$ semi-rational.

- GENERAL PROPERTIES
- The following are equivalent:

1. $x \in G$ semi-rational.
2. $\exists$ a positive integer m_0 such that every generator of $\langle x \rangle$ is conjugate in G to either x or x^{m_0}.

- GENERAL PROPERTIES
- The following are equivalent:

1. $x \in G$ semi-rational.
2. $\exists$ a positive integer m_0 such that every generator of $\langle x \rangle$ is conjugate in G to either x or x^{m_0}.
3. $\left| \frac{N_G(<x>)}{C_G(x)} \right| = \phi(|x|)$ or $\frac{1}{2}\phi(|x|)$.

- GENERAL PROPERTIES
- The following are equivalent:

1. $x \in G$ semi-rational.
2. $\exists$ a positive integer m_0 such that every generator of $\langle x \rangle$ is conjugate in G to either x or x^{m_0}.
3. $\left| \frac{N_G(<x>)}{C_G(x)} \right| = \phi(|x|)$ or $\frac{1}{2}\phi(|x|)$.

- Furthermore: $x \in G$ semi-rational $\Rightarrow$ (**but not equivalent to)** $\chi(x)$ lies in a quadratic extension of $\mathbb{Q}$ for all $\chi \in Irr(G)$.

- Characterization of semi-rational groups in terms of their "characters field of value", would be helpful. We do not have such. If G is rational then so is G/N for $N \lhd G$, because $Irr(G/N) \subset Irr(G)$. The same is true for "semi-rational", except that we do not have immediate "character reason", maybe because the lack of a "field of values" characterization.

- Characterization of semi-rational groups in terms of their "characters field of value", would be helpful. We do not have such. If G is rational then so is G/N for $N \lhd G$, because $Irr(G/N) \subset Irr(G)$. The same is true for "semi-rational", except that we do not have immediate "character reason", maybe because the lack of a "field of values" characterization.

Lemma

If G is semi-rational, then so is G/N.

- PROOF.Let $xN \in G/N$ and $x_0 \in xN$ of minimal order. Semi-rationality $\Rightarrow \exists m_0$ such that if $\langle z \rangle = \langle x_0 \rangle$ then z is congugate to eiher x_0 or $x_0^{m_0}$.

- PROOF.Let $xN \in G/N$ and $x_0 \in xN$ of minimal order. Semi-rationality $\Rightarrow \exists m_0$ such that if $\langle z\rangle = \langle x_0\rangle$ then z is congugate to eiher x_0 or $x_0^{m_0}$.
- Assume $\langle xN\rangle = \langle yN\rangle$ $(= \langle x_0 N\rangle)$. Then $\exists a, b$ with $(xN)^a = yN$ and $(yN)^b = xN$. So

$$(x_0)^a \in yN \quad , (x_0)^{ab} \in (yN)^b = xN.$$

- PROOF.Let $xN \in G/N$ and $x_0 \in xN$ of minimal order. Semi-rationality $\Rightarrow \exists m_0$ such that if $\langle z \rangle = \langle x_0 \rangle$ then z is congugate to eiher x_0 or $x_0^{m_0}$.
- Assume $\langle xN \rangle = \langle yN \rangle$ $(= \langle x_0 N \rangle)$. Then $\exists a, b$ with $(xN)^a = yN$ and $(yN)^b = xN$. So

$$(x_0)^a \in yN \quad , (x_0)^{ab} \in (yN)^b = xN.$$

- Minimality of $|x_0| \Rightarrow \left|x_0^{ab}\right| = |x_0| \Rightarrow \langle x_0^a \rangle = \langle x_0 \rangle$.

- PROOF.Let $xN \in G/N$ and $x_0 \in xN$ of minimal order. Semi-rationality $\Rightarrow \exists m_0$ such that if $\langle z \rangle = \langle x_0 \rangle$ then z is congugate to eiher x_0 or $x_0^{m_0}$.
- Assume $\langle xN \rangle = \langle yN \rangle$ $(= \langle x_0 N \rangle)$. Then $\exists a, b$ with $(xN)^a = yN$ and $(yN)^b = xN$. So

$$(x_0)^a \in yN \quad , (x_0)^{ab} \in (yN)^b = xN.$$

- Minimality of $|x_0| \Rightarrow \left|x_0^{ab}\right| = |x_0| \Rightarrow \langle x_0^a \rangle = \langle x_0 \rangle$.
- So $\exists g$ such that $(x_0^a)^g = x_0$ or $(x_0)^{m_0}$ $\Rightarrow (yN)^g = (x_0^a N)^g = \begin{cases} x_0 N = xN \\ x_0^{m_0} N = x^{m_0} N \end{cases}.$

- **OUTLINE OF PROOF OF MAIN THEOREM.** The proof uses some of the Gow's paper techniques and methods from Eelena Farias Soares paper "Big primes and character values for solvable groups" (1986).

- **OUTLINE OF PROOF OF MAIN THEOREM**. The proof uses some of the Gow's paper techniques and methods from Eelena Farias Soares paper "Big primes and character values for solvable groups" (1986).
- Let G be semi-rational solvable group. We induct on $|G|$.

- **OUTLINE OF PROOF OF MAIN THEOREM**. The proof uses some of the Gow's paper techniques and methods from Eelena Farias Soares paper "Big primes and character values for solvable groups" (1986).
- Let G be semi-rational solvable group. We induct on $|G|$.
- INITIAL REDUCTION. Let $V \lhd G$ be minimal normal $\Rightarrow$ V is an elementary abelian p - group, p a prime. Induction $\Rightarrow \pi(G/V) \subset \{2, 3, 5, 7, 13, 17\}$. May assume: $p \notin \{2, 3, 5, 7, 13, 17\}$ and that V is the unique minimal normal subgroup of G. So $G = HV$ a semi-direct product, and V is an irreducible faithfull H - module.

- We illustrate the proof for $p = 19$. The proof for $p = 1 + 2^a 3^b$ with $b > 1$ is similar. Will not talk on how to show that $p = 1 + 2^a 3^b$ (follows as an indirect application of Soares' main reault). Will not on how to proof that $b \leq 4$.

- We illustrate the proof for $p = 19$. The proof for $p = 1 + 2^a 3^b$ with $b > 1$ is similar. Will not talk on how to show that $p = 1 + 2^a 3^b$ (follows as an indirect application of Soares' main reault). Will not on how to proof that $b \leq 4$.
- Let $v \in V - \{1\}$. Then $|Aut\langle v\rangle| = 18$. Semirationality $\Leftrightarrow \frac{N_G(<v>)}{C_G(v)}$ is (isomorphic to) a subgroup of index 1 or 2 of $Aut\langle v\rangle$.

- We illustrate the proof for $p = 19$. The proof for $p = 1 + 2^a 3^b$ with $b > 1$ is similar. Will not talk on how to show that $p = 1 + 2^a 3^b$ (follows as an indirect application of Soares' main reault). Will not on how to proof that $b \leq 4$.
- Let $v \in V - \{1\}$. Then $|Aut\langle v \rangle| = 18$. Semirationality $\Leftrightarrow \frac{N_G(<v>)}{C_G(v)}$ is (isomorphic to) a subgroup of index 1 or 2 of $Aut\langle v \rangle$.
- Identify $Aut\langle v \rangle$ with $\mathbb{F} = GF(19)$. Let $\mu \in \mathbb{F}$ be of order 9.

- We illustrate the proof for $p = 19$. The proof for $p = 1 + 2^a 3^b$ with $b > 1$ is similar. Will not talk on how to show that $p = 1 + 2^a 3^b$ (follows as an indirect application of Soares' main reault). Will not on how to proof that $b \leq 4$.
- Let $v \in V - \{1\}$. Then $|Aut\langle v\rangle| = 18$. Semirationality $\Leftrightarrow \frac{N_G(<v>)}{C_G(v)}$ is (isomorphic to) a subgroup of index 1 or 2 of $Aut\langle v\rangle$.
- Identify $Aut\langle v\rangle$ with $\mathbb{F} = GF(19)$. Let $\mu \in \mathbb{F}$ be of order 9.
- Semirationality $\Rightarrow$ elements of ordr 9 of $Aut\langle v\rangle$ must lie in $\frac{N_G(<v>)}{C_G(v)}$, and some $g \in N_G(< v >)$ of order 9 mod $C_G(v)$, satisfies $vg = \mu v$ (using additive notation: vg for v^g).

- As $G = VH$ and V abelian, may assume $g \in H$. So the action of H on V has the following property: (*) $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.

- As $G = VH$ and V abelian, may assume $g \in H$. So the action of H on V has the following property: (*) $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.
- SECOND REDUCTION By a method devised by E. Farias Soares (1986), H and V can be replaced by "new" ones such that H now acts on V with no fixed points , and most of relevant properties of the original H and V are unchanged. In particular (*), and "$\chi(x)$ belongs to some quadratic extension of the rationals, for all $\chi \in Irr(G)$" remsin true.

- As $G = VH$ and V abelian, may assume $g \in H$. So the action of H on V has the following property: (*) $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.
- SECOND REDUCTION By a method devised by E. Farias Soares (1986), H and V can be replaced by "new" ones such that H now acts on V with no fixed points , and most of relevant properties of the original H and V are unchanged. In particular (*), and "$\chi(x)$ belongs to some quadratic extension of the rationals, for all $\chi \in Irr(G)$" remsin true.
- We do however, lose semi-rationality.

- So far:

- So far:
  1. H a Frobenius complement.

- So far:
  1. H a Frobenius complement.
  2. $\pi(|H|) \subset \{2,3,5,7,13,17\}$

- So far:
  1. H a Frobenius complement.
  2. $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$
  3. H acts on the elememntary abelian 19 - group V with no fixed points.

- So far:

1. H a Frobenius complement.
2. $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$
3. H acts on the elememntary abelian 19 - group V with no fixed points.
4. (*) For $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.

- So far:
  1. H a Frobenius complement.
  2. $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$
  3. H acts on the elememntary abelian 19 - group V with no fixed points.
  4. (*) For $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.
- Set $|V| = 19^n$.

- So far:

  1. H a Frobenius complement.
  2. $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$
  3. H acts on the elememntary abelian 19 - group V with no fixed points.
  4. (*) For $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.

- Set $|V| = 19^n$.
- Let $X = \{x \in H \mid |x| = 9\}$ and $W_x = \{v \in V \mid vx = \mu v\}$ (the μ - eigenspace of x in V).

- So far:
  1. H a Frobenius complement.
  2. $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$
  3. H acts on the elememntary abelian 19 - group V with no fixed points.
  4. (*) For $\forall \mu \in \mathbb{F}$ of order 9 and every $v \in V$, $\exists g \in H$ of order 9 such that $vg = \mu v$.
- Set $|V| = 19^n$.
- Let $X = \{x \in H \mid |x| = 9\}$ and $W_x = \{v \in V \mid vx = \mu v\}$ (the μ - eigenspace of x in V).
- (*) $\Rightarrow V = \bigcup_{x \in X} W_x \Rightarrow 19^n \leq \sum_{x \in X} |W_x|$.

- Counting argumnets.

- Counting argumnets.
    1. Using "$\chi(x)$ belongs to some quadratic extension of the rationals, for all $x \in Irr(G)$" and an application of another result of Soares, we get that $n = 3f$ and $\dim(W_x) \leq f$ for all $x \in X$.
    So $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f\,|X| \Rightarrow 19^{2f} \leq |X|$.

- Counting argumnets.

  1. Using "$\chi(x)$ belongs to some quadratic extension of the rationals, for all $x \in Irr(G)$" and an application of another result of Soares, we get that $n = 3f$ and $\dim(W_x) \leq f$ for all $x \in X$.
     So $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$.
  2. Bounding $|X|$. H as Frobenius complement has a well known structure. Recall that $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$. Not hard to show that X lies in some normal subgroup M whose $\{7, 13\}$-Hall subgroup D is cyclic. Then it can be shown that $|X| \leq 24d$ where $d = |D|$.

- Counting argumnets.

1. Using "$\chi(x)$ belongs to some quadratic extension of the rationals, for all $x \in Irr(G)$" and an application of another result of Soares, we get that $n = 3f$ and $\dim(W_x) \leq f$ for all $x \in X$.
   So $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$.
2. Bounding $|X|$. H as Frobenius complement has a well known structure. Recall that $\pi(|H|) \subset \{2, 3, 5, 7, 13, 17\}$. Not hard to show that X lies in some normal subgroup M whose $\{7, 13\}$-Hall subgroup D is cyclic. Then it can be shown that $|X| \leq 24d$ where $d = |D|$.
3. $\phi(d)$ divides $12f$.

- $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f\,|X| \Rightarrow 19^{2f} \leq |X|$
  $\Rightarrow 19^{2f} \leq 24d.$

- $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$
$\Rightarrow 19^{2f} \leq 24d.$
- $d \geq \frac{19^2}{24} = 15.04 \Rightarrow d \geq 16$. So $\pi(d) = \{7, 13\}$
$\Rightarrow d \geq 49$

- $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$
  $\Rightarrow 19^{2f} \leq 24d.$
- $d \geq \frac{19^2}{24} = 15.04 \Rightarrow d \geq 16$. So $\pi(d) = \{7, 13\}$
  $\Rightarrow d \geq 49$
- Set $d = 7^\alpha \cdot 13^\beta$. Then $\phi(d) = \frac{7^\alpha \cdot 13^\beta}{7 \cdot 13} \cdot 6 \cdot 12$
  $= d \cdot \frac{72}{91} \geq \frac{7}{9} d$. $\left(\frac{72}{91} - \frac{7}{9} = 0.0134\right)$.

- $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$
  $\Rightarrow 19^{2f} \leq 24d.$
- $d \geq \frac{19^2}{24} = 15.04 \Rightarrow d \geq 16.$ So $\pi(d) = \{7, 13\}$
  $\Rightarrow d \geq 49$
- Set $d = 7^\alpha \cdot 13^\beta$. Then $\phi(d) = \frac{7^\alpha \cdot 13^\beta}{7 \cdot 13} \cdot 6 \cdot 12$
  $= d \cdot \frac{72}{91} \geq \frac{7}{9} d.$ $\left(\frac{72}{91} - \frac{7}{9} = 0.0134\right).$
- $\phi(d)$ divides $12f \Rightarrow 2f \geq \frac{\phi(d)}{6} \geq \frac{7}{9 \cdot 6} d.$

- $19^n \leq \sum_{x \in X} |W_x| \Rightarrow 19^{3f} \leq 19^f |X| \Rightarrow 19^{2f} \leq |X|$
  $\Rightarrow 19^{2f} \leq 24d.$
- $d \geq \frac{19^2}{24} = 15.04 \Rightarrow d \geq 16.$ So $\pi(d) = \{7, 13\}$
  $\Rightarrow d \geq 49$
- Set $d = 7^\alpha \cdot 13^\beta$. Then $\phi(d) = \frac{7^\alpha \cdot 13^\beta}{7 \cdot 13} \cdot 6 \cdot 12$
  $= d \cdot \frac{72}{91} \geq \frac{7}{9} d.$ $\left(\frac{72}{91} - \frac{7}{9} = 0.0134\right).$
- $\phi(d)$ divides $12f \Rightarrow 2f \geq \frac{\phi(d)}{6} \geq \frac{7}{9 \cdot 6} d.$
- $24d \geq 19^{2f} \geq 19^{\frac{7}{54} d}$. Impossible for $d \geq 49$.