Norm Invariance method and Applications

Kristijan Tabak
Rochester Institute of Technology
kxtcad@rit.edu
joint work with M.O. Pavčević

ALCOMA 15, March 2015

Definition

A (v, k, λ) difference set in a finite group G of order v is a set D, of cardinality k, such that the collection $\{d_1 d_2^{-1} \mid d_1 \neq d_2,\ d_i \in D\}$ consists of λ copies of every element of $G \setminus \{1_G\}$.

Definition

A (v, k, λ) difference set in a finite group G of order v is a set D, of cardinality k, such that the collection $\{d_1 d_2^{-1} \mid d_1 \neq d_2,\ d_i \in D\}$ consists of λ copies of every element of $G \setminus \{1_G\}$.

Theorem

If D is a (v, k, λ) difference set in G then $DD^{(-1)} = (k - \lambda)1_G + \lambda G$ holds in group ring $\mathbb{Z}[G]$.

Definition

A (v, k, λ) difference set in a finite group G of order v is a set D, of cardinality k, such that the collection $\{d_1 d_2^{-1} \mid d_1 \neq d_2,\ d_i \in D\}$ consists of λ copies of every element of $G \setminus \{1_G\}$.

Theorem

If D is a (v, k, λ) difference set in G then $DD^{(-1)} = (k - \lambda)1_G + \lambda G$ holds in group ring $\mathbb{Z}[G]$.

If a 2-group possesses a difference set, then its parameter set is $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$. We shall call such a set **Hadamard difference set** and the group in which it is contained **Hadamard group**.

Definition

A (v, k, λ) difference set in a finite group G of order v is a set D, of cardinality k, such that the collection $\{d_1 d_2^{-1} \mid d_1 \neq d_2,\ d_i \in D\}$ consists of λ copies of every element of $G \setminus \{1_G\}$.

Theorem

If D is a (v, k, λ) difference set in G then $DD^{(-1)} = (k - \lambda)1_G + \lambda G$ holds in group ring $\mathbb{Z}[G]$.

If a 2-group possesses a difference set, then its parameter set is $(2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d)$. We shall call such a set **Hadamard difference set** and the group in which it is contained **Hadamard group**.

Example (abelian)

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ be the elementary abelian group of order 16. Its subset

$$\begin{aligned} D &= \{(0,0,0,0), (1,0,0,0), (0,1,0,0), \\ &\quad (0,0,1,0), (0,0,0,1), (1,1,1,1)\} \end{aligned}$$

is a $(16, 6, 2)$ difference set, which can be verified easily.

Example (abelian)

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ be the elementary abelian group of order 16. Its subset

$$\begin{aligned} D &= \{(0,0,0,0), (1,0,0,0), (0,1,0,0), \\ &\quad (0,0,1,0), (0,0,0,1), (1,1,1,1)\} \end{aligned}$$

is a $(16,6,2)$ difference set, which can be verified easily.

Example (nonabelian)

Let $M_{16} = \langle x, y \mid x^8 = y^2 = 1,\ yxy = x^5 \rangle$ be the modular group of order 16. Then

$$D = 1 + x + x^2 + x^5 + x^4 y + x^2 y$$

is a $(16,6,2)$ difference set in nonabelian group

Example (abelian)

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ be the elementary abelian group of order 16. Its subset

$$\begin{aligned} D &= \{(0,0,0,0), (1,0,0,0), (0,1,0,0), \\ &\quad (0,0,1,0), (0,0,0,1), (1,1,1,1)\} \end{aligned}$$

is a $(16,6,2)$ difference set, which can be verified easily.

Example (nonabelian)

Let $M_{16} = \langle x, y \mid x^8 = y^2 = 1,\ yxy = x^5 \rangle$ be the modular group of order 16. Then

$$D = 1 + x + x^2 + x^5 + x^4 y + x^2 y$$

is a $(16,6,2)$ difference set in nonabelian group

$DD^{(-1)} = (1+x+x^2+x^5+x^4y+x^2y)(1+x^7+x^6+x^3+yx^4+yx^6) =$

$$= 4 \cdot 1_{M_{16}} + 2M_{16}$$

Example (abelian)

Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ be the elementary abelian group of order 16. Its subset

$$\begin{aligned} D \;=\; \{&(0,0,0,0),\,(1,0,0,0),\,(0,1,0,0),\\ &(0,0,1,0),\,(0,0,0,1),\,(1,1,1,1)\} \end{aligned}$$

is a $(16, 6, 2)$ difference set, which can be verified easily.

Example (nonabelian)

Let $M_{16} = \langle x, y \mid x^8 = y^2 = 1,\ yxy = x^5\rangle$ be the modular group of order 16. Then

$$D = 1 + x + x^2 + x^5 + x^4y + x^2y$$

is a $(16, 6, 2)$ difference set in nonabelian group

$DD^{(-1)} = (1+x+x^2+x^5+x^4y+x^2y)(1+x^7+x^6+x^3+yx^4+yx^6) =$

$$= 4 \cdot 1_{M_{16}} + 2M_{16}$$

Theorem: An abelian group of order 2^{2d+2} contains a Hadamard difference set if and only if the exponent of G is at the most 2^{d+2}.

Theorem: An abelian group of order 2^{2d+2} contains a Hadamard difference set if and only if the exponent of G is at the most 2^{d+2}.

Theorem: Let D be a subset of size k of a group G of order v. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. Then, $\phi(D)\phi(D^{(-1)}) = (k - \lambda)I$ for all $\phi \in S$, if and only if D is a (v, k, λ) difference set in G.

Theorem: An abelian group of order 2^{2d+2} contains a Hadamard difference set if and only if the exponent of G is at the most 2^{d+2}.

Theorem: Let D be a subset of size k of a group G of order v. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. Then, $\phi(D)\phi(D^{(-1)}) = (k-\lambda)I$ for all $\phi \in S$, if and only if D is a (v, k, λ) difference set in G.

Theorem (Turyn): Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is cyclic. If $|H| < 2^d$ then G is not a Hadamard group.

Theorem: An abelian group of order 2^{2d+2} contains a Hadamard difference set if and only if the exponent of G is at the most 2^{d+2}.

Theorem: Let D be a subset of size k of a group G of order v. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. Then, $\phi(D)\phi(D^{(-1)}) = (k-\lambda)I$ for all $\phi \in S$, if and only if D is a (v, k, λ) difference set in G.

Theorem (Turyn): Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is cyclic. If $|H| < 2^d$ then G is not a Hadamard group.

Theorem (Ma) Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is dihedral. If $|H| < 2^d$ then G is not a Hadamard group.

Theorem: An abelian group of order 2^{2d+2} contains a Hadamard difference set if and only if the exponent of G is at the most 2^{d+2}.

Theorem: Let D be a subset of size k of a group G of order v. Let S be a complete set of distinct, inequivalent, nontrivial, irreducible representations for G. Then, $\phi(D)\phi(D^{(-1)}) = (k-\lambda)I$ for all $\phi \in S$, if and only if D is a (v, k, λ) difference set in G.

Theorem (Turyn): Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is cyclic. If $|H| < 2^d$ then G is not a Hadamard group.

Theorem (Ma) Let G be a 2-group of order 2^{2d+2}, and H a normal subgroup such that G/H is dihedral. If $|H| < 2^d$ then G is not a Hadamard group.

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

$$\begin{aligned} D &= 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + \\ &\quad x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} + \\ &\quad y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y + \\ &\quad x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y. \end{aligned}$$

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

$$\begin{aligned} D \;=\; & 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + \\ & x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} + \\ & y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y + \\ & x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y. \end{aligned}$$

The modular group defined in terms of generators and relations as:

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

$$\begin{aligned} D \;=\; & 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + \\ & x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} + \\ & y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y + \\ & x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y. \end{aligned}$$

The modular group defined in terms of generators and relations as:

$$M_{2^{2d+2}} = \langle x, y \mid x^{2^{2d+1}} = y^2 = 1,\ x^y = x^{2^{2d}+1} \rangle$$

has representations of dimensions 1 and 2.

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

$$\begin{aligned} D \;=\; & 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + \\ & x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} + \\ & y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y + \\ & x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y. \end{aligned}$$

The modular group defined in terms of generators and relations as:

$$M_{2^{2d+2}} = \langle x, y \mid x^{2^{2d+1}} = y^2 = 1,\ x^y = x^{2^{2d}+1} \rangle$$

has representations of dimensions 1 and 2.
The reason is: if a group G has an abelian subgroup A, and $\rho : G \to GL(V)$ is irreducible representation, then $dim(V) \leq [G : A]$.

Example Have a look at the modular group or order 64, $M_{64} = \langle x, y \mid x^{32} = y^2 = 1,\ yxy = x^{17} \rangle$ and a $(64, 28, 12)$ difference set D found in it, found by K. Smith:

$$\begin{aligned} D \;=\; & 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} + \\ & x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} + \\ & y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y + \\ & x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y. \end{aligned}$$

The modular group defined in terms of generators and relations as:

$$M_{2^{2d+2}} = \langle x, y \mid x^{2^{2d+1}} = y^2 = 1,\ x^y = x^{2^{2d}+1} \rangle$$

has representations of dimensions 1 and 2.
The reason is: if a group G has an abelian subgroup A, and $\rho : G \to GL(V)$ is irreducible representation, then $dim(V) \leq [G : A]$.

1−dimensional representations are
$\varphi_{ks}(x^m y^s) = \varepsilon^{2mk}(-1)^{ls},\ \varepsilon = \exp\left(\frac{2\pi i}{2^{2d+1}}\right),$
$k = 0, 1, 2, \ldots, 2^{2d+1} - 1,\ l = 0, 1$

1−dimensional representations are
$\varphi_{ks}(x^m y^s) = \varepsilon^{2mk}(-1)^{ls}, \ \varepsilon = \exp\left(\frac{2\pi i}{2^{2d+1}}\right),$
$k = 0, 1, 2, \ldots, 2^{2d+1} - 1, \ l = 0, 1$

Therefore, if D is a difference set in $M_{2^{2d+2}}$, then it is Hadamard difference set and

1−dimensional representations are
$\varphi_{ks}(x^m y^s) = \varepsilon^{2mk}(-1)^{ls},\ \varepsilon = \exp\left(\frac{2\pi i}{2^{2d+1}}\right),$
$k = 0, 1, 2, \ldots, 2^{2d+1} - 1,\ l = 0, 1$

Therefore, if D is a difference set in $M_{2^{2d+2}}$, then it is Hadamard difference set and

$$\varphi_{ks}(D)\varphi_{ks}(D^{(-1)}) = \varphi_{ks}(D)\overline{\varphi_{ks}(D)} = |\varphi_{ks}(D)|^2 = 2^{2d}.$$

1−dimensional representations are
$\varphi_{ks}(x^m y^s) = \varepsilon^{2mk}(-1)^{ls},\ \varepsilon = \exp\left(\frac{2\pi i}{2^{2d+1}}\right),$
$k = 0, 1, 2, \ldots, 2^{2d+1} - 1,\ l = 0, 1$

Therefore, if D is a difference set in $M_{2^{2d+2}}$, then it is Hadamard difference set and

$$\varphi_{ks}(D)\varphi_{ks}(D^{(-1)}) = \varphi_{ks}(D)\overline{\varphi_{ks}(D)} = |\varphi_{ks}(D)|^2 = 2^{2d}.$$

Have a look again at the difference set D in M_{64}:

1−dimensional representations are
$\varphi_{ks}(x^m y^s) = \varepsilon^{2mk}(-1)^{ls},\ \varepsilon = \exp\left(\frac{2\pi i}{2^{2d+1}}\right),$
$k = 0, 1, 2, \ldots, 2^{2d+1} - 1,\ l = 0, 1$

Therefore, if D is a difference set in $M_{2^{2d+2}}$, then it is Hadamard difference set and

$$\varphi_{ks}(D)\varphi_{ks}(D^{(-1)}) = \varphi_{ks}(D)\overline{\varphi_{ks}(D)} = |\varphi_{ks}(D)|^2 = 2^{2d}.$$

Have a look again at the difference set D in M_{64}:

$$D = 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} +$$
$$+ x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} +$$
$$y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y +$$
$$x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y$$

$$D = 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} +$$
$$+ x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} +$$
$$y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y +$$
$$x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y$$

Look at 15 homomorphisms $\varphi_{k0} : M_{64} \to \mathbb{C}$ which act as:

$$\varphi_{k0}(x) = \varepsilon^{2k}, \quad \varphi_{k0}(y) = 1, \quad k = 1, \ldots, 15, \quad \varepsilon^{32} = 1.$$

$$D = 1 + x + x^2 + x^3 + x^4 + x^6 + x^9 + x^{10} +$$
$$+ x^{11} + x^{13} + x^{16} + x^{17} + x^{20} + x^{21} + x^{25} + x^{30} +$$
$$y + x^6 y + x^{12} y + x^{13} y + x^{16} y + x^{18} y +$$
$$x^{19} y + x^{21} y + x^{26} y + x^{27} y + x^{28} y + x^{30} y$$

Look at 15 homomorphisms $\varphi_{k0} : M_{64} \to \mathbb{C}$ which act as:

$$\varphi_{k0}(x) = \varepsilon^{2k}, \quad \varphi_{k0}(y) = 1, \quad k = 1, \ldots, 15, \quad \varepsilon^{32} = 1.$$

One can easily compute:

$$
\begin{aligned}
\varphi_{10}(D) &= 1+\varepsilon^2+\varepsilon^4+\varepsilon^6+\varepsilon^8+\varepsilon^{12}+\varepsilon^{18}+\varepsilon^{20}+ \\
&+ \varepsilon^{22}+\varepsilon^{26}+\varepsilon^{32}+\varepsilon^{34}+\varepsilon^{40}+\varepsilon^{42}+\varepsilon^{50}+\varepsilon^{60}+ \\
&+ 1+\varepsilon^{12}+\varepsilon^{24}+\varepsilon^{26}+\varepsilon^{32}+\varepsilon^{36}+ \\
&+ \varepsilon^{38}+\varepsilon^{42}+\varepsilon^{52}+\varepsilon^{54}+\varepsilon^{56}+\varepsilon^{60} \\
&= 4+2\varepsilon^2+2\varepsilon^4+2\varepsilon^6+2\varepsilon^8+2\varepsilon^{10}+2\varepsilon^{12}+ \\
&+ +2\varepsilon^{18}+2\varepsilon^{20}+2\varepsilon^{22}+2\varepsilon^{24}+2\varepsilon^{26}+2\varepsilon^{28} \\
&= 4+2(1+\varepsilon^{16})(\varepsilon^2+\varepsilon^4+\varepsilon^6+\varepsilon^8+\varepsilon^{10}+\varepsilon^{12}) = 4.
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{20}(D) &= 1+\varepsilon^4+\varepsilon^8+\varepsilon^{12}+\varepsilon^{16}+\varepsilon^{24}+\varepsilon^{36}+\varepsilon^{40}+ \\
&+ \varepsilon^{44}+\varepsilon^{52}+\varepsilon^{64}+\varepsilon^{68}+\varepsilon^{80}+\varepsilon^{84}+\varepsilon^{100}+\varepsilon^{120}+ \\
&+ 1+\varepsilon^{24}+\varepsilon^{48}+\varepsilon^{52}+\varepsilon^{64}+\varepsilon^{72}+ \\
&+ \varepsilon^{76}+\varepsilon^{84}+\varepsilon^{104}+\varepsilon^{108}+\varepsilon^{112}+\varepsilon^{120} \\
&= 4+4\varepsilon^4+4\varepsilon^8+4\varepsilon^{12}+4\varepsilon^{16}+4\varepsilon^{20}+4\varepsilon^{24}+ \\
&= 4\varepsilon^{12}+4(1+\varepsilon^{16})(1+\varepsilon^4+\varepsilon^8)=4\varepsilon^{12}.
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{20}(D) &= 1+\varepsilon^4+\varepsilon^8+\varepsilon^{12}+\varepsilon^{16}+\varepsilon^{24}+\varepsilon^{36}+\varepsilon^{40}+ \\
&+ \varepsilon^{44}+\varepsilon^{52}+\varepsilon^{64}+\varepsilon^{68}+\varepsilon^{80}+\varepsilon^{84}+\varepsilon^{100}+\varepsilon^{120}+ \\
&+ 1+\varepsilon^{24}+\varepsilon^{48}+\varepsilon^{52}+\varepsilon^{64}+\varepsilon^{72}+ \\
&+ \varepsilon^{76}+\varepsilon^{84}+\varepsilon^{104}+\varepsilon^{108}+\varepsilon^{112}+\varepsilon^{120} \\
&= 4+4\varepsilon^4+4\varepsilon^8+4\varepsilon^{12}+4\varepsilon^{16}+4\varepsilon^{20}+4\varepsilon^{24}+ \\
&= 4\varepsilon^{12}+4(1+\varepsilon^{16})(1+\varepsilon^4+\varepsilon^8)=4\varepsilon^{12}.
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{40}(D) &= 1+\varepsilon^{8}+\varepsilon^{16}+\varepsilon^{24}+\varepsilon^{32}+\varepsilon^{48}+\varepsilon^{72}+\varepsilon^{80}+\\
&+ \varepsilon^{88}+\varepsilon^{104}+\varepsilon^{128}+\varepsilon^{136}+\varepsilon^{160}+\varepsilon^{168}+\varepsilon^{200}+\varepsilon^{240}+\\
&+ 1+\varepsilon^{48}+\varepsilon^{96}+\varepsilon^{104}+\varepsilon^{128}+\varepsilon^{144}+\\
&+ \varepsilon^{152}+\varepsilon^{168}+\varepsilon^{208}+\varepsilon^{216}+\varepsilon^{224}+\varepsilon^{240}\\
&= 8+8\varepsilon^{8}+8\varepsilon^{16}+4\varepsilon^{24}\\
&= 4\varepsilon^{8}+(1+\varepsilon^{16})(8+4\varepsilon^{8})=4\varepsilon^{8}.
\end{aligned}
$$

The same is true if we look at another set of 15 homomorphisms $\varphi_{k1} : M_{64} \to \mathbb{C}$ which act as:

$$\varphi_{k1}(x) = \varepsilon^{2k}, \quad \varphi_{k1}(y) = -1, \quad k = 1, \ldots, 15, \quad \varepsilon^{32} = 1,$$

The same is true if we look at another set of 15 homomorphisms $\varphi_{k1} : M_{64} \to \mathbb{C}$ which act as:

$$\varphi_{k1}(x) = \varepsilon^{2k}, \quad \varphi_{k1}(y) = -1, \quad k = 1, \ldots, 15, \quad \varepsilon^{32} = 1,$$

for example

$$\begin{aligned}
\varphi_{11}(D) &= 1 + \varepsilon^2 + \varepsilon^4 + \varepsilon^6 + \varepsilon^8 + \varepsilon^{12} + \varepsilon^{18} + \varepsilon^{20} + \\
&+ \varepsilon^{22} + \varepsilon^{26} + \varepsilon^{32} + \varepsilon^{34} + \varepsilon^{40} + \varepsilon^{42} + \varepsilon^{50} + \varepsilon^{60} + \\
&+ \varepsilon^{16} + \varepsilon^{28} + \varepsilon^{40} + \varepsilon^{42} + \varepsilon^{48} + \varepsilon^{52} + \\
&+ \varepsilon^{54} + \varepsilon^{58} + \varepsilon^{68} + \varepsilon^{70} + \varepsilon^{72} + \varepsilon^{76} \\
&= 2 + 2\varepsilon^2 + 2\varepsilon^4 + 2\varepsilon^6 + 4\varepsilon^8 + 2\varepsilon^{10} + 2\varepsilon^{12} + \\
&+ +2\varepsilon^{16} + 2\varepsilon^{18} + 2\varepsilon^{20} + 2\varepsilon^{22} + 2\varepsilon^{26} + 2\varepsilon^{28} \\
&= 4\varepsilon^8 + 2(1 + \varepsilon^{16})(1 + \varepsilon^2 + \varepsilon^4 + \varepsilon^6 + \varepsilon^{10} + \varepsilon^{12}) = 4\varepsilon^8.
\end{aligned}$$

The same is true if we look at another set of 15 homomorphisms $\varphi_{k1} : M_{64} \to \mathbb{C}$ which act as:

$$\varphi_{k1}(x) = \varepsilon^{2k}, \quad \varphi_{k1}(y) = -1, \quad k = 1, \dots, 15, \quad \varepsilon^{32} = 1,$$

for example

$$\begin{aligned}
\varphi_{11}(D) &= 1 + \varepsilon^2 + \varepsilon^4 + \varepsilon^6 + \varepsilon^8 + \varepsilon^{12} + \varepsilon^{18} + \varepsilon^{20} + \\
&+ \varepsilon^{22} + \varepsilon^{26} + \varepsilon^{32} + \varepsilon^{34} + \varepsilon^{40} + \varepsilon^{42} + \varepsilon^{50} + \varepsilon^{60} + \\
&+ \varepsilon^{16} + \varepsilon^{28} + \varepsilon^{40} + \varepsilon^{42} + \varepsilon^{48} + \varepsilon^{52} + \\
&+ \varepsilon^{54} + \varepsilon^{58} + \varepsilon^{68} + \varepsilon^{70} + \varepsilon^{72} + \varepsilon^{76} \\
&= 2 + 2\varepsilon^2 + 2\varepsilon^4 + 2\varepsilon^6 + 4\varepsilon^8 + 2\varepsilon^{10} + 2\varepsilon^{12} + \\
&+ +2\varepsilon^{16} + 2\varepsilon^{18} + 2\varepsilon^{20} + 2\varepsilon^{22} + 2\varepsilon^{26} + 2\varepsilon^{28} \\
&= 4\varepsilon^8 + 2(1 + \varepsilon^{16})(1 + \varepsilon^2 + \varepsilon^4 + \varepsilon^6 + \varepsilon^{10} + \varepsilon^{12}) = 4\varepsilon^8.
\end{aligned}$$

Definition Let ε be a root of unity and $f(\varepsilon) = \sum_{j=1}^{w} k_j \varepsilon^{r_j} \in \mathbb{Z}[\varepsilon]$. If there is some c, such that $|f(\varepsilon^p)| = c$, for all integers p, then we say that $f(\varepsilon)$ is **norm invariant**, of norm c.

Definition Let ε be a root of unity and $f(\varepsilon) = \sum_{j=1}^{w} k_j \varepsilon^{r_j} \in \mathbb{Z}[\varepsilon]$. If there is some c, such that $|f(\varepsilon^p)| = c$, for all integers p, then we say that $f(\varepsilon)$ is **norm invariant**, of norm c.

Theorem (pairwise abbreviation) Let $\varepsilon = e^{\frac{2\pi i}{2^k}}$, $n \geq 1$. Suppose that $\varepsilon^{\alpha_1} + \varepsilon^{\alpha_2} + \cdots + \varepsilon^{\alpha_l} = 0$. Then l is even and there is a partition of the set $\{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ in 2-element subsets $\{\alpha_i, \alpha_j\}$ such that $\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0$.

Definition Let ε be a root of unity and $f(\varepsilon) = \sum_{j=1}^{w} k_j \varepsilon^{r_j} \in \mathbb{Z}[\varepsilon]$. If there is some c, such that $|f(\varepsilon^p)| = c$, for all integers p, then we say that $f(\varepsilon)$ is **norm invariant**, of norm c.

Theorem (pairwise abbreviation) Let $\varepsilon = e^{\frac{2\pi i}{2^k}}$, $n \geq 1$. Suppose that $\varepsilon^{\alpha_1} + \varepsilon^{\alpha_2} + \cdots + \varepsilon^{\alpha_l} = 0$. Then l is even and there is a partition of the set $\{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ in 2-element subsets $\{\alpha_i, \alpha_j\}$ such that $\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0$.

Lemma (about four roots) Let $\eta^{r_i},\ i = 1, 2, 3, 4$ are four different roots, and $o(\eta) = 2^n,\ n \geq 1$, then $|\eta^{x_1} + \eta^{x_2} + \eta^{x_3} + \eta^{x_4}| \neq 2$.

Definition Let ε be a root of unity and $f(\varepsilon) = \sum_{j=1}^{w} k_j \varepsilon^{r_j} \in \mathbb{Z}[\varepsilon]$. If there is some c, such that $|f(\varepsilon^p)| = c$, for all integers p, then we say that $f(\varepsilon)$ is **norm invariant**, of norm c.

Theorem (pairwise abbreviation) Let $\varepsilon = e^{\frac{2\pi i}{2^k}}$, $n \geq 1$. Suppose that $\varepsilon^{\alpha_1} + \varepsilon^{\alpha_2} + \cdots + \varepsilon^{\alpha_l} = 0$. Then l is even and there is a partition of the set $\{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ in 2-element subsets $\{\alpha_i, \alpha_j\}$ such that $\varepsilon^{\alpha_i} + \varepsilon^{\alpha_j} = 0$.

Lemma (about four roots) Let $\eta^{r_i},\ i = 1, 2, 3, 4$ are four different roots, and $o(\eta) = 2^n,\ n \geq 1$, then $|\eta^{x_1} + \eta^{x_2} + \eta^{x_3} + \eta^{x_4}| \neq 2$.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Notice that assumption leads to $|G'| < 2^d$.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Notice that assumption leads to $|G'| < 2^d$.

Take $G/G' = \displaystyle\prod_{j=1}^{t} \langle g_j G' \rangle \cong \prod_{j=1}^{t} \langle \varepsilon_j \rangle$

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Notice that assumption leads to $|G'| < 2^d$.

Take $G/G' = \prod_{j=1}^{t} \langle g_j G' \rangle \cong \prod_{j=1}^{t} \langle \varepsilon_j \rangle$

where $\varepsilon_j = exp\left(\frac{2\pi i}{2^{s_j}}\right),\ j \in [t]$.

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Notice that assumption leads to $|G'| < 2^d$.

Take $G/G' = \prod_{j=1}^{t} \langle g_j G' \rangle \cong \prod_{j=1}^{t} \langle \varepsilon_j \rangle$

where $\varepsilon_j = exp\left(\frac{2\pi i}{2^{s_j}}\right),\ j \in [t]$.

For any χ in dual group $\widehat{G/G'}$

Theorem (norm invariance) Let $f(\eta) = \eta^{r_1} + \cdots + \eta^{r_q}$ be a norm invariant polynomial of norm 2^d where $q = 2^d(2^{d+1} - 1)$ and η is a root of unity of order 2^{2d+2}. Let $2^n = max\{o(\eta^{r_i})\}$. Then for every $k = 0, 1, 2, \ldots, n-1$ there is an $r_{(k)} \in \mathbb{Z}$ such that $f(\eta^{2^k}) = 2^d \eta^{r_{(k)}}$. We call such polynomials $f(\eta^{2^k})$ maximally abbreviated.

Let G be a group of order 2^{2d+2} and $|G : G'| > 2^{d+2}$.

Clearly $G' \trianglelefteq G$.

Notice that assumption leads to $|G'| < 2^d$.

Take $G/G' = \prod_{j=1}^{t} \langle g_j G' \rangle \cong \prod_{j=1}^{t} \langle \varepsilon_j \rangle$

where $\varepsilon_j = exp\left(\frac{2\pi i}{2^{s_j}}\right), \ j \in [t]$.

For any χ in dual group $\widehat{G/G'}$

we can write

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}$ for some integer α_j's.

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}$ for some integer α_j's.

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}} : G \to C$ by

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}$ for some integer α_j's.

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}} : G \to C$ by

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}}(g_1^{\beta_1}g_2^{\beta_2}\dots g_t^{\beta_t}h) = \varepsilon_1^{\alpha_1\beta_1}\varepsilon_2^{\alpha_2\beta_2}\cdots\varepsilon_t^{\alpha_t\beta_t}.$

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}$ for some integer α_j's.

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}} : G \to C$ by

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}}(g_1^{\beta_1}g_2^{\beta_2}\ldots g_t^{\beta_t}h) = \varepsilon_1^{\alpha_1\beta_1}\varepsilon_2^{\alpha_2\beta_2}\cdots\varepsilon_t^{\alpha_t\beta_t}.$

Put $|G/G'| = 2^s$ and

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}$ for some integer α_j's.

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}} : G \to C$ by

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}}(g_1^{\beta_1}g_2^{\beta_2}\dots g_t^{\beta_t}h) = \varepsilon_1^{\alpha_1\beta_1}\varepsilon_2^{\alpha_2\beta_2}\cdots\varepsilon_t^{\alpha_t\beta_t}$.

Put $|G/G'| = 2^s$ and

$$D = \bigsqcup_{k=0}^{2^s-1}(D \cap a_k G') = \bigsqcup_{k=0}^{2^s-1}\{a_k h_1, a_k h_2, \dots, a_k h_{w_k}\}.$$

we can write

$\chi = \chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}$ for some integer α_j's.

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}} : G \to C$ by

$\varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}}(g_1^{\beta_1}g_2^{\beta_2}\dots g_t^{\beta_t}h) = \varepsilon_1^{\alpha_1\beta_1}\varepsilon_2^{\alpha_2\beta_2}\cdots\varepsilon_t^{\alpha_t\beta_t}$.

Put $|G/G'| = 2^s$ and

$$D = \bigsqcup_{k=0}^{2^s-1}(D \cap a_k G') = \bigsqcup_{k=0}^{2^s-1}\{a_k h_1, a_k h_2, \dots, a_k h_{w_k}\}.$$

Clearly, $w_k \geq 0$ and $w_k \leq |G'| < 2^d$.

we have

we have

$$\varphi_\chi(D) = \sum_{k=0}^{2^s-1} w_k \varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}}(g_1^{\beta_{1k}} g_2^{\beta_{2k}} \dots g_t^{\beta_{tk}} h) =$$

$$\sum_{k=0}^{2^s-1} w_k \varepsilon_1^{\alpha_1\beta_{1k}} \varepsilon_2^{\alpha_2\beta_{2k}} \cdots \varepsilon_t^{\alpha_t\beta_{tk}},$$

we have

$$\varphi_\chi(D) = \sum_{k=0}^{2^s-1} w_k \varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}}(g_1^{\beta_{1k}} g_2^{\beta_{2k}} \ldots g_t^{\beta_{tk}} h) =$$

$$\sum_{k=0}^{2^s-1} w_k \varepsilon_1^{\alpha_1\beta_{1k}} \varepsilon_2^{\alpha_2\beta_{2k}} \cdots \varepsilon_t^{\alpha_t\beta_{tk}},$$

where $a_k = \prod_{j=1}^{t} g_j^{\beta_{jk}}$.

we have

$$\varphi_\chi(D) = \sum_{k=0}^{2^s-1} w_k \varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\ldots\chi_t^{\alpha_t}}(g_1^{\beta_{1k}} g_2^{\beta_{2k}} \ldots g_t^{\beta_{tk}} h) =$$

$$\sum_{k=0}^{2^s-1} w_k \varepsilon_1^{\alpha_1\beta_{1k}} \varepsilon_2^{\alpha_2\beta_{2k}} \cdots \varepsilon_t^{\alpha_t\beta_{tk}},$$

where $a_k = \prod_{j=1}^{t} g_j^{\beta_{jk}}$.

Thus, because of $|\varphi_\chi(D)| = 2^d$ we have

we have

$$\varphi_\chi(D) = \sum_{k=0}^{2^s-1} w_k \varphi_{\chi_1^{\alpha_1}\chi_2^{\alpha_2}\dots\chi_t^{\alpha_t}}(g_1^{\beta_{1k}} g_2^{\beta_{2k}} \dots g_t^{\beta_{tk}} h) =$$

$$\sum_{k=0}^{2^s-1} w_k \varepsilon_1^{\alpha_1\beta_{1k}} \varepsilon_2^{\alpha_2\beta_{2k}} \cdots \varepsilon_t^{\alpha_t\beta_{tk}},$$

where $a_k = \prod_{j=1}^{t} g_j^{\beta_{jk}}$.

Thus, because of $|\varphi_\chi(D)| = 2^d$ we have

$$\left|\sum_{k=0}^{2^s-1} w_k \varepsilon_1^{\alpha_1\beta_{1k}} \varepsilon_2^{\alpha_2\beta_{2k}} \cdots \varepsilon_t^{\alpha_t\beta_{tk}}\right| = 2^d,$$

Now, we can take for example

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

thus there must be some w_k such that $w_k \geq 2^d$. A contradiction.

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

thus there must be some w_k such that $w_k \geq 2^d$. A contradiction.

Theorem: Let G be a group of order 2^{2d+2}. If $|G : G'| > 2^{d+2}$, then G is not a Hadamard group.

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

thus there must be some w_k such that $w_k \geq 2^d$. A contradiction.

Theorem: Let G be a group of order 2^{2d+2}. If $|G : G'| > 2^{d+2}$, then G is not a Hadamard group.

If $H \trianglelefteq G$ such that $|G| = 2^{2d+2}$ and $|H| < 2^d$ and G/H is cyclic,

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

thus there must be some w_k such that $w_k \geq 2^d$. A contradiction.

Theorem: Let G be a group of order 2^{2d+2}. If $|G : G'| > 2^{d+2}$, then G is not a Hadamard group.

If $H \trianglelefteq G$ such that $|G| = 2^{2d+2}$ and $|H| < 2^d$ and G/H is cyclic,

then $G' \leq H$ (because G/H is abelian),

Now, we can take for example

$\alpha_1 = \alpha_2 = \cdots = \alpha_{t-1} = 0$, while $\alpha_t \neq 0$

and still we get norm invariant polynomial in one variable,

thus there must be some w_k such that $w_k \geq 2^d$. A contradiction.

Theorem: Let G be a group of order 2^{2d+2}. If $|G : G'| > 2^{d+2}$, then G is not a Hadamard group.

If $H \trianglelefteq G$ such that $|G| = 2^{2d+2}$ and $|H| < 2^d$ and G/H is cyclic,

then $G' \leq H$ (because G/H is abelian),

and by previous result we have claim of cyclic case.