Mass formulas for self-dual codes

Akihiro MUNEMASA (宗政昭弘)

Graduate School of Information Sciences
Tohoku University 東北大学
(joint work with Rowena A. L. Betty)

Self-dual, self-orthogonal codes

- R : finite commutative ring
- n : positive integer
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, for $x, y \in R^n$
- C : R-submodule of R^n
- $C^\perp = \{x \in R^n \mid (x, y) = 0 \text{ for all } y \in C\}$
- C : self-dual if $C = C^\perp$
- C : self-orthogonal if $C \subset C^\perp$

Self-dual, self-orthogonal codes

- R : finite commutative ring
- n : positive integer
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, for $x, y \in R^n$
- C : R-submodule of R^n
- $C^\perp = \{x \in R^n \mid (x, y) = 0 \text{ for all } y \in C\}$
- C : self-dual if $C = C^\perp$
- C : self-orthogonal if $C \subset C^\perp$

Self-dual, self-orthogonal codes

- R : finite commutative ring
- n : positive integer
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, for $x, y \in R^n$
- C : R-submodule of R^n
- $C^\perp = \{x \in R^n \mid (x, y) = 0 \text{ for all } y \in C\}$
- C : self-dual if $C = C^\perp$
- C : self-orthogonal if $C \subset C^\perp$

Self-dual, self-orthogonal codes

- R : finite commutative ring
- n : positive integer
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, for $x, y \in R^n$
- C : R-submodule of R^n
- $C^\perp = \{x \in R^n \mid (x, y) = 0 \text{ for all } y \in C\}$
- C : self-dual if $C = C^\perp$
- C : self-orthogonal if $C \subset C^\perp$

Self-dual, self-orthogonal codes

- R : finite commutative ring
- n : positive integer
- $(x, y) = \sum_{i=1}^{n} x_i y_i$, for $x, y \in R^n$
- C : R-submodule of R^n
- $C^\perp = \{x \in R^n \mid (x, y) = 0 \text{ for all } y \in C\}$
- C : self-dual if $C = C^\perp$
- C : self-orthogonal if $C \subset C^\perp$

Mass formulas

The number of self-dual codes of length n

- over $\mathbb{F}_p$ (the number of maximal totally isotropic subspaces, the index of a maximal parabolic subgroup in a finite classical group) is known for years.
- over $\mathbb{Z}_4$: was given by Gaborit (1996).

Mass formula $=$ a formula giving the number of certain (self-dual or self-orthogonal, for instance) codes of length n over a ring R.

Mass formulas

The number of self-dual codes of length n

- over $\mathbb{F}_p$ (the number of maximal totally isotropic subspaces, the index of a maximal parabolic subgroup in a finite classical group) is known for years.
- over $\mathbb{Z}_4$: was given by Gaborit (1996).

Mass formula $=$ a formula giving the number of certain (self-dual or self-orthogonal, for instance) codes of length n over a ring R.

More mass formulas

	$\mathbb{Z}_{p^2}$	$\mathbb{Z}_{p^3}$	$\mathbb{Z}_{p^m}$
s.d.	BBN	NNW	?
s.o.	BM	?	?

	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{2^m}$
s.d.	G	NNW	?
s.o.	BM	?	?
even s.d.	G	?	?
even s.o.	BM*	?	?

G Gaborit, 1996
BBN Balmaceda–Betty–Nemenzo, 2008
BM Betty–Munemasa, submitted
NNW Nagata–Nemenzo–Wada, preprint
* $\mathbf{1} \in C_1$, $n \equiv 0 \pmod 8$.

More mass formulas

	$\mathbb{Z}_{p^2}$	$\mathbb{Z}_{p^3}$	$\mathbb{Z}_{p^m}$
s.d.	BBN	NNW	?
s.o.	BM	?	?

	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{2^m}$
s.d.	G	NNW	?
s.o.	BM	?	?
even s.d.	G	?	?
even s.o.	BM*	?	?

G Gaborit, 1996

BBN Balmaceda–Betty–Nemenzo, 2008

BM Betty–Munemasa, submitted

NNW Nagata–Nemenzo–Wada, preprint

* $\mathbf{1} \in C_1$, $n \equiv 0 \pmod 8$.

Mass formula for even self-dual codes over $\mathbb{Z}_8$

In particular, we want to verify our numerical result (with M. Harada) on

the number of 8-frames in the E_8-lattice

$$= 45{,}102{,}825 \quad \text{(by computer)}$$

$$= \frac{|\operatorname{Aut}(E_8)|}{2^8 \cdot 8!} \cdot \#\text{ even self-dual codes of length 8 over } \mathbb{Z}_8$$

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

The number of (not necessarily even) self-dual codes over $\mathbb{Z}_8$ is due to Nagata–Nemenzo–Wada.

Mass formula for even self-dual codes over $\mathbb{Z}_8$

In particular, we want to verify our numerical result (with M. Harada) on

the number of 8-frames in the E_8-lattice

$$= 45{,}102{,}825 \quad \text{(by computer)}$$

$$= \frac{|\mathrm{Aut}(E_8)|}{2^8 \cdot 8!} \cdot \#\text{ even self-dual codes of length 8 over } \mathbb{Z}_8$$

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

The number of (not necessarily even) self-dual codes over $\mathbb{Z}_8$ is due to Nagata–Nemenzo–Wada.

Mass formula for even self-dual codes over $\mathbb{Z}_8$

In particular, we want to verify our numerical result (with M. Harada) on

the number of 8-frames in the E_8-lattice

$$= 45{,}102{,}825 \quad \text{(by computer)}$$

$$= \frac{|\operatorname{Aut}(E_8)|}{2^8 \cdot 8!} \cdot \#\text{ even self-dual codes of length 8 over } \mathbb{Z}_8$$

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

The number of (not necessarily even) self-dual codes over $\mathbb{Z}_8$ is due to Nagata–Nemenzo–Wada.

Mass formula for even self-dual codes over $\mathbb{Z}_8$

In particular, we want to verify our numerical result (with M. Harada) on

the number of 8-frames in the E_8-lattice

$$= 45{,}102{,}825 \quad \text{(by computer)}$$

$$= \frac{|\mathrm{Aut}(E_8)|}{2^8 \cdot 8!} \cdot \#\ \text{even self-dual codes of length 8 over } \mathbb{Z}_8$$

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

The number of (not necessarily even) self-dual codes over $\mathbb{Z}_8$ is due to Nagata–Nemenzo–Wada.

Mass formula for even self-dual codes over $\mathbb{Z}_8$

In particular, we want to verify our numerical result (with M. Harada) on

the number of 8-frames in the E_8-lattice

$= 45{,}102{,}825$ (by computer)

$= \dfrac{|\operatorname{Aut}(E_8)|}{2^8 \cdot 8!} \cdot \#$ even self-dual codes of length 8 over $\mathbb{Z}_8$

$$\theta_{E_8} = 1 + 240q + 2160q^2 + 6720q^3 + 17520q^4 + \cdots$$

The number of (not necessarily even) self-dual codes over $\mathbb{Z}_8$ is due to Nagata–Nemenzo–Wada.

Technique: from $\mathbb{F}_p$-codes to $\mathbb{Z}_{p^2}$-codes

- C_1: self-orthogonal code over $\mathbb{F}_p$.
- want to count #self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that $C \bmod p = C_1$ (residue of C).

If C_1 has generator matrix A, then C has generator matrix

$$\begin{bmatrix} A + pN \\ pB \end{bmatrix}$$

for some N, B.

In what follows, generator matrices of codes will have integer entries.

Technique: from $\mathbb{F}_p$-codes to $\mathbb{Z}_{p^2}$-codes

- C_1: self-orthogonal code over $\mathbb{F}_p$.
- want to count #self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that $C \bmod p = C_1$ (residue of C).

If C_1 has generator matrix A, then C has generator matrix

$$\begin{bmatrix} A + pN \\ pB \end{bmatrix}$$

for some N, B.

In what follows, generator matrices of codes will have integer entries.

Technique: from $\mathbb{F}_p$-codes to $\mathbb{Z}_{p^2}$-codes

- C_1: self-orthogonal code over $\mathbb{F}_p$.
- want to count #self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that C mod $p = C_1$ (residue of C).

If C_1 has generator matrix A, then C has generator matrix

$$\begin{bmatrix} A + pN \\ pB \end{bmatrix}$$

for some N, B.
In what follows, generator matrices of codes will have integer entries.

Technique: from $\mathbb{F}_p$-codes to $\mathbb{Z}_{p^2}$-codes

- C_1: self-orthogonal code over $\mathbb{F}_p$.
- want to count #self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that C mod $p = C_1$ (residue of C).

If C_1 has generator matrix A, then C has generator matrix

$$\begin{bmatrix} A + pN \\ pB \end{bmatrix}$$

for some N, B.

In what follows, generator matrices of codes will have integer entries.

Technique: from $\mathbb{F}_p$-codes to $\mathbb{Z}_{p^2}$-codes

- C_1: self-orthogonal code over $\mathbb{F}_p$.
- want to count #self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that C mod $p = C_1$ (residue of C).

If C_1 has generator matrix A, then C has generator matrix

$$\begin{bmatrix} A + pN \\ pB \end{bmatrix}$$

for some N, B.
In what follows, generator matrices of codes will have integer entries.

Free codes

- C_1: self-orthogonal code over $\mathbb{F}_p$ with generator matrix $\begin{bmatrix} I & A \end{bmatrix}$.
- want to count # free self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that C mod $p = C_1$.

C : free

$\iff$ $C \cong \mathbb{Z}_{p^2}^k$, where $k = \dim C_1$

$\iff$ C has generator matrix $\begin{bmatrix} I + pN_1 & A + pN_2 \end{bmatrix}$

$\iff$ C has generator matrix $\begin{bmatrix} I & A + pN \end{bmatrix}$

N is uniquely determined by C.

Free codes

- C_1: self-orthogonal code over $\mathbb{F}_p$ with generator matrix $\begin{bmatrix} I & A \end{bmatrix}$.
- want to count # free self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that C mod $p = C_1$.

C : free

$\iff C \cong \mathbb{Z}_{p^2}^k$, where $k = \dim C_1$

$\iff C$ has generator matrix $\begin{bmatrix} I + pN_1 & A + pN_2 \end{bmatrix}$

$\iff C$ has generator matrix $\begin{bmatrix} I & A + pN \end{bmatrix}$

N is uniquely determined by C.

Free codes

- C_1: self-orthogonal code over $\mathbb{F}_p$ with generator matrix $\begin{bmatrix} I & A \end{bmatrix}$.
- want to count $\#$ free self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that $C \bmod p = C_1$.

C : free

$$\iff C \cong \mathbb{Z}_{p^2}^k, \text{ where } k = \dim C_1$$
$$\iff C \text{ has generator matrix } \begin{bmatrix} I + pN_1 & A + pN_2 \end{bmatrix}$$
$$\iff C \text{ has generator matrix } \begin{bmatrix} I & A + pN \end{bmatrix}$$

N is uniquely determined by C.

Free codes

- C_1: self-orthogonal code over $\mathbb{F}_p$ with generator matrix $\begin{bmatrix} I & A \end{bmatrix}$.
- want to count # free self-orthogonal codes C over $\mathbb{Z}_{p^2}$ such that $C \bmod p = C_1$.

C : free

$$\iff C \cong \mathbb{Z}_{p^2}^k, \text{ where } k = \dim C_1$$
$$\iff C \text{ has generator matrix } \begin{bmatrix} I + pN_1 & A + pN_2 \end{bmatrix}$$
$$\iff C \text{ has generator matrix } \begin{bmatrix} I & A + pN \end{bmatrix}$$

N is uniquely determined by C.

Free codes with given residue

$C_1 : \begin{bmatrix} I & A \end{bmatrix} / \mathbb{F}_p$, $I + AA^T \equiv 0 \pmod p$, C: $\begin{bmatrix} I & A + pN \end{bmatrix} / \mathbb{Z}_{p^2}$.

- C is self-orthogonal $\iff$ $I + AA^T + p(AN^T + NA^T) \equiv 0 \pmod{p^2}$.

So

$$\#C = \#N \text{ s.t. } AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p.$$

In general,

$$\#\{N \mid AN^T + NA^T \equiv \text{given} \pmod p\} = ?$$

Note $\mathrm{rank}_p A = k$, since $I + AA^T \equiv 0 \pmod p$.

Free codes with given residue

$C_1 : [I \quad A] \,/\mathbb{F}_p$, $\quad I + AA^T \equiv 0 \pmod p$, $\quad C$: $[I \quad A + pN] \,/\mathbb{Z}_{p^2}$.

- C is self-orthogonal $\iff$
  $I + AA^T + p(AN^T + NA^T) \equiv 0 \pmod{p^2}$.

So

$$\#C = \#N \text{ s.t. } AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p.$$

In general,

$$\#\{N \mid AN^T + NA^T \equiv \text{given} \pmod p\} = ?$$

Note $\operatorname{rank}_p A = k$, since $I + AA^T \equiv 0 \pmod p$.

Free codes with given residue

$C_1 : [I \quad A] \ /\mathbb{F}_p, \quad I + AA^T \equiv 0 \pmod p, \quad C\colon [I \quad A + pN] \ /\mathbb{Z}_{p^2}.$

- C is self-orthogonal $\iff$
  $I + AA^T + p(AN^T + NA^T) \equiv 0 \pmod{p^2}$.

So

$$\#C = \#N \text{ s.t. } AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p.$$

In general,

$$\#\{N \mid AN^T + NA^T \equiv \text{given} \pmod p\} = ?$$

Note $\text{rank}_p A = k$, since $I + AA^T \equiv 0 \pmod p$.

Free codes with given residue

$C_1 : [I \quad A] / \mathbb{F}_p, \quad I + AA^T \equiv 0 \pmod{p}, \quad C\colon [I \quad A + pN] / \mathbb{Z}_{p^2}.$

- C is self-orthogonal $\iff$
  $I + AA^T + p(AN^T + NA^T) \equiv 0 \pmod{p^2}.$

So

$$\#C = \#N \text{ s.t. } AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod{p}.$$

In general,

$$\#\{N \mid AN^T + NA^T \equiv \text{given} \pmod{p}\} = ?$$

Note $\mathrm{rank}_p A = k$, since $I + AA^T \equiv 0 \pmod{p}$.

Free codes with given residue

$C_1 : [I \quad A] \ /\mathbb{F}_p, \quad I + AA^T \equiv 0 \pmod{p}, \quad C\!: [I \quad A + pN] \ /\mathbb{Z}_{p^2}.$

- C is self-orthogonal $\iff$ $I + AA^T + p(AN^T + NA^T) \equiv 0 \pmod{p^2}$.

So

$$\#C = \#N \text{ s.t. } AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod{p}.$$

In general,

$$\#\{N \mid AN^T + NA^T \equiv \text{given} \pmod{p}\} = ?$$

Note $\mathrm{rank}_p A = k$, since $I + AA^T \equiv 0 \pmod{p}$.

Mapping on matrices

$\#N$ s.t. $AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p$

$$\begin{array}{cccc} \Psi : & M_{k\times m}(\mathbb{F}_p) & \to & \mathrm{Sym}_k(\mathbb{F}_p) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_p)$, $\operatorname{rank} A = k$.

Lemma

p: odd prime $\Longrightarrow$ Ψ: surjective.

$$\begin{aligned} &\#\{N \mid AN^T + NA^T = \text{given}\} \\ &= \#\Psi^{-1}(\text{given}) = \#\operatorname{Ker}\Psi \\ &= p^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Sym}_k(\mathbb{F}_p)} = p^{km-k(k+1)/2}. \end{aligned}$$

Mapping on matrices

$\#N$ s.t. $AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_p) & \to & \mathrm{Sym}_k(\mathbb{F}_p) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_p)$, rank $A = k$.

Lemma

p: odd prime $\implies$ Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given}\}$$
$$= \#\Psi^{-1}(\text{given}) = \#\operatorname{Ker}\Psi$$
$$= p^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Sym}_k(\mathbb{F}_p)} = p^{km-k(k+1)/2}.$$

Mapping on matrices

$\#N$ s.t. $AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod{p}$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_p) & \to & \mathrm{Sym}_k(\mathbb{F}_p) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_p)$, rank $A = k$.

Lemma

p: odd prime $\implies$ Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given}\}$$
$$= \#\Psi^{-1}(\text{given}) = \#\operatorname{Ker}\Psi$$
$$= p^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Sym}_k(\mathbb{F}_p)} = p^{km-k(k+1)/2}.$$

Mapping on matrices

$\# N$ s.t. $AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod{p}$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_p) & \to & \mathrm{Sym}_k(\mathbb{F}_p) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_p)$, rank $A = k$.

Lemma

p: odd prime $\Longrightarrow$ Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given}\}$$
$$= \#\Psi^{-1}(\text{given}) = \#\operatorname{Ker}\Psi$$
$$= p^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Sym}_k(\mathbb{F}_p)} = p^{km - k(k+1)/2}.$$

Mapping on matrices

$\#N$ s.t. $AN^T + NA^T \equiv -\frac{1}{p}(I + AA^T) \pmod p$

$$\begin{array}{rccc} \Psi: & M_{k\times m}(\mathbb{F}_p) & \to & \mathrm{Sym}_k(\mathbb{F}_p) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_p)$, rank $A = k$.

Lemma

p: odd prime $\implies \Psi$: surjective.

$$\begin{aligned} &\#\{N \mid AN^T + NA^T = \text{given}\} \\ &= \#\Psi^{-1}(\text{given}) = \#\operatorname{Ker}\Psi \\ &= p^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Sym}_k(\mathbb{F}_p)} = p^{km - k(k+1)/2}. \end{aligned}$$

$p = 2$, $\Psi : N \mapsto AN^T + NA^T \in \mathrm{Sym}_k(\mathbb{F}_p)$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Alt}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_2)$, rank $A = k$.

Lemma

Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given} \in \mathrm{Alt}_k(\mathbb{F}_p)\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Alt}_k(\mathbb{F}_p)}$$
$$= 2^{km - k(k-1)/2}.$$

$p = 2$, $\Psi : N \mapsto AN^T + NA^T \in \mathrm{Sym}_k(\mathbb{F}_p)$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Alt}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_2)$, rank $A = k$.

Lemma

Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given} \in \mathrm{Alt}_k(\mathbb{F}_p)\}$$
$$= \#\operatorname{Ker}\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Alt}_k(\mathbb{F}_p)}$$
$$= 2^{km - k(k-1)/2}.$$

$p = 2$, $\Psi : N \mapsto AN^T + NA^T \in \mathrm{Sym}_k(\mathbb{F}_p)$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Alt}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_2)$, rank $A = k$.

Lemma

Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given} \in \mathrm{Alt}_k(\mathbb{F}_p)\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Alt}_k(\mathbb{F}_p)}$$
$$= 2^{km - k(k-1)/2}.$$

$p = 2$, $\Psi : N \mapsto AN^T + NA^T \in \mathrm{Sym}_k(\mathbb{F}_p)$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Alt}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_2)$, rank $A = k$.

Lemma

Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given} \in \mathrm{Alt}_k(\mathbb{F}_p)\}$$
$$= \#\operatorname{Ker}\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Alt}_k(\mathbb{F}_p)}$$
$$= 2^{km-k(k-1)/2}.$$

$p = 2$, $\Psi : N \mapsto AN^T + NA^T \in \mathrm{Sym}_k(\mathbb{F}_p)$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Alt}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T \end{array}$$

where $A \in M_{k\times m}(\mathbb{F}_2)$, rank $A = k$.

Lemma

Ψ: surjective.

$$\#\{N \mid AN^T + NA^T = \text{given} \in \mathrm{Alt}_k(\mathbb{F}_p)\}$$
$$= \# \operatorname{Ker} \Psi = 2^{\dim M_{k\times m}(\mathbb{F}_p) - \dim \mathrm{Alt}_k(\mathbb{F}_p)}$$
$$= 2^{km - k(k-1)/2}.$$

Even codes over $\mathbb{Z}_4$

$C_1 : [I \quad A] \,/\mathbb{F}_2, \quad C: [I \quad A + 2N] \,/\mathbb{Z}_4.$

Problem

- When is C even (i.e., Euclidean norm (weight)$\equiv 0 \pmod 8$)?
- Count $\#N$ for which C is even.

In addition to C being self-orthogonal, i.e.,

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

we need:

$$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$$

Even codes over $\mathbb{Z}_4$

$C_1 : [I \quad A] \ /\mathbb{F}_2, \quad C: [I \quad A + 2N] \ /\mathbb{Z}_4.$

Problem

- When is C even (i.e., Euclidean norm (weight)$\equiv 0 \pmod 8$)?
- Count $\#N$ for which C is even.

In addition to C being self-orthogonal, i.e.,

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

we need:

$$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$$

Even codes over $\mathbb{Z}_4$

$C_1 : [I \quad A] \ /\mathbb{F}_2, \quad C: [I \quad A + 2N] \ /\mathbb{Z}_4.$

Problem

- When is C even (i.e., Euclidean norm (weight)$\equiv 0 \pmod 8$)?
- Count $\# N$ for which C is even.

In addition to C being self-orthogonal, i.e.,

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

we need:

$$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$$

Even codes over $\mathbb{Z}_4$

$C_1 : [I \quad A] \ /\mathbb{F}_2, \quad C\colon [I \quad A + 2N] \ /\mathbb{Z}_4.$

Problem

- When is C even (i.e., Euclidean norm (weight)$\equiv 0 \pmod 8$)?
- Count $\#N$ for which C is even.

In addition to C being self-orthogonal, i.e.,

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

we need:

$$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$$

Even codes over $\mathbb{Z}_4$

$C_1 : [I \quad A] \ /\mathbb{F}_2, \quad C: [I \quad A+2N] \ /\mathbb{Z}_4.$

Problem

- When is C even (i.e., Euclidean norm (weight)$\equiv 0 \pmod 8$)?
- Count $\#N$ for which C is even.

In addition to C being self-orthogonal, i.e.,

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

we need:

$$\mathrm{Diag}(I+AA^T+2(AN^T+NA^T)+4NN^T) \equiv 0 \pmod 8.$$

$$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$$

$$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$$

$$AN^T + NA^T \equiv \frac{1}{2}(I + AA^T) \pmod 2$$

$$\mathrm{Diag}(I + AA^T + 4AN^T + 4NN^T) \equiv 0 \pmod 8,$$

$$\frac{1}{4}\mathrm{Diag}(I + AA^T) \equiv \mathrm{Diag}(AN^T + NN^T) \pmod 2$$

$$\equiv \mathrm{Diag}((A + J)N^T) \pmod 2.$$

$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$

$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$

$$AN^T + NA^T \equiv \frac{1}{2}(I + AA^T) \pmod 2$$

$$\mathrm{Diag}(I + AA^T + 4AN^T + 4NN^T) \equiv 0 \pmod 8,$$

$$\frac{1}{4}\mathrm{Diag}(I + AA^T) \equiv \mathrm{Diag}(AN^T + NN^T) \pmod 2$$

$$\equiv \mathrm{Diag}((A + J)N^T) \pmod 2.$$

$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$

$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$

$$AN^T + NA^T \equiv \frac{1}{2}(I + AA^T) \pmod 2$$

$$\mathrm{Diag}(I + AA^T + 4AN^T + 4NN^T) \equiv 0 \pmod 8,$$

$$\frac{1}{4}\mathrm{Diag}(I + AA^T) \equiv \mathrm{Diag}(AN^T + NN^T) \pmod 2$$

$$\equiv \mathrm{Diag}((A + J)N^T) \pmod 2.$$

$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4$,

$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8$.

$$AN^T + NA^T \equiv \frac{1}{2}(I + AA^T) \pmod 2$$

$$\mathrm{Diag}(I + AA^T + 4AN^T + 4NN^T) \equiv 0 \pmod 8,$$

$$\frac{1}{4}\mathrm{Diag}(I + AA^T) \equiv \mathrm{Diag}(AN^T + NN^T) \pmod 2$$

$$\equiv \mathrm{Diag}((A + J)N^T) \pmod 2.$$

$I + AA^T + 2(AN^T + NA^T) \equiv 0 \pmod 4,$

$\mathrm{Diag}(I + AA^T + 2(AN^T + NA^T) + 4NN^T) \equiv 0 \pmod 8.$

$$AN^T + NA^T \equiv \frac{1}{2}(I + AA^T) \pmod 2$$

$$\mathrm{Diag}(I + AA^T + 4AN^T + 4NN^T) \equiv 0 \pmod 8,$$

$$\frac{1}{4}\mathrm{Diag}(I + AA^T) \equiv \mathrm{Diag}(AN^T + NN^T) \pmod 2$$

$$\equiv \mathrm{Diag}((A + J)N^T) \pmod 2.$$

$$AN^T + NA^T \equiv \text{given} \pmod 2,$$

$$\mathrm{Diag}((A+J)N^T) \equiv \text{given} \pmod 2.$$

$$\begin{array}{rccc} \Psi : & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Sym}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T + \mathrm{Diag}((A+J)N^T) \end{array}$$

Lemma

Ψ: surjective if $1 \notin C_1 = \mathrm{span}\begin{bmatrix} I & A \end{bmatrix}$.

$$\#\{N \mid AN^T + NA^T = \text{given},\ \mathrm{Diag}((A+J)N^T) = \text{given}\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_2) - \dim \mathrm{Sym}_k(\mathbb{F}_2)}$$
$$= 2^{km - k(k+1)/2}.$$

$AN^T + NA^T \equiv \text{given} \pmod 2,$

$\mathrm{Diag}((A+J)N^T) \equiv \text{given} \pmod 2.$

$$\begin{array}{cccc} \Psi: & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Sym}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T + \mathrm{Diag}((A+J)N^T) \end{array}$$

Lemma

Ψ: surjective if $1 \notin C_1 = \mathrm{span}\begin{bmatrix} I & A \end{bmatrix}$.

$$\#\{N \mid AN^T + NA^T = \text{given},\ \mathrm{Diag}((A+J)N^T) = \text{given}\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_2) - \dim \mathrm{Sym}_k(\mathbb{F}_2)}$$
$$= 2^{km - k(k+1)/2}.$$

$AN^T + NA^T \equiv \text{given} \pmod 2,$

$\text{Diag}((A+J)N^T) \equiv \text{given} \pmod 2.$

$$\begin{array}{rccc} \Psi: & M_{k\times m}(\mathbb{F}_2) & \to & \text{Sym}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T + \text{Diag}((A+J)N^T) \end{array}$$

Lemma

Ψ: surjective if $\mathbf{1} \notin C_1 = \text{span}\begin{bmatrix} I & A \end{bmatrix}$.

$\#\{N \mid AN^T + NA^T = \text{given},\ \text{Diag}((A+J)N^T) = \text{given}\}$

$= \#\,\text{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_2) - \dim \text{Sym}_k(\mathbb{F}_2)}$

$= 2^{km - k(k+1)/2}.$

$AN^T + NA^T \equiv \text{given} \pmod 2,$

$\mathrm{Diag}((A+J)N^T) \equiv \text{given} \pmod 2.$

$$\begin{array}{rccc} \Psi: & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Sym}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T + \mathrm{Diag}((A+J)N^T) \end{array}$$

Lemma

Ψ: surjective if $\mathbf{1} \notin C_1 = \mathrm{span}\begin{bmatrix} I & A \end{bmatrix}$.

$$\#\{N \mid AN^T + NA^T = \text{given}, \ \mathrm{Diag}((A+J)N^T) = \text{given}\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_2) - \dim \mathrm{Sym}_k(\mathbb{F}_2)}$$
$$= 2^{km - k(k+1)/2}.$$

$AN^T + NA^T \equiv \text{given} \pmod 2,$

$\mathrm{Diag}((A+J)N^T) \equiv \text{given} \pmod 2.$

$$\begin{array}{rccc} \Psi: & M_{k\times m}(\mathbb{F}_2) & \to & \mathrm{Sym}_k(\mathbb{F}_2) \\ & N & \mapsto & AN^T + NA^T + \mathrm{Diag}((A+J)N^T) \end{array}$$

Lemma

Ψ: surjective if $\mathbf{1} \notin C_1 = \text{span}\begin{bmatrix} I & A \end{bmatrix}$.

$$\#\{N \mid AN^T + NA^T = \text{given},\ \mathrm{Diag}((A+J)N^T) = \text{given}\}$$
$$= \#\,\mathrm{Ker}\,\Psi = 2^{\dim M_{k\times m}(\mathbb{F}_2) - \dim \mathrm{Sym}_k(\mathbb{F}_2)}$$
$$= 2^{km - k(k+1)/2}.$$

More mass formulas

	$\mathbb{Z}_{p^2}$	$\mathbb{Z}_{p^3}$	$\mathbb{Z}_{p^m}$
s.d.	BBN	NNW	?
s.o.	BM	?	?

	$\mathbb{Z}_4$	$\mathbb{Z}_8$	$\mathbb{Z}_{2^m}$
s.d.	G	NNW	?
s.o.	BM	?	?
even s.d.	G	?	?
even s.o.	BM*	?	?

G Gaborit, 1996

BBN Balmaceda–Betty–Nemenzo, to appear

BM Betty–Munemasa, submitted

NNW Nagata–Nemenzo–Wada, preprint

* $\mathbf{1} \in C_1$, $n \equiv 0 \pmod 8$.