A short survey on perfect codes in Cayley graphs

Sanming Zhou

School of Mathematics and Statistics
The University of Melbourne
Australia

International Workshop on Symmetries of Graph and Networks, 29/1/2018, Sanya
A code is perfect if it achieves maximum possible error correction without ambiguity.

$C$ is a perfect $t$-code if it has covering radius $t$ and minimum distance $2t + 1$ (with respect to the Hamming distance).

$C$ is a perfect $t$-code iff every word of length $n$ is at distance no more than $t$ to exactly one codeword of $C$. 
perfect codes in the classical setting

- A code is perfect if it achieves maximum possible error correction without ambiguity.
- $C$ is a perfect $t$-code if it has covering radius $t$ and minimum distance $2t + 1$ (with respect to the Hamming distance).
- $C$ is a perfect $t$-code iff every word of length $n$ is at distance no more than $t$ to exactly one codeword of $C$. 
A code is perfect if it achieves maximum possible error correction without ambiguity.

C is a perfect $t$-code if it has covering radius $t$ and minimum distance $2t + 1$ (with respect to the Hamming distance).

$C$ is a perfect $t$-code iff every word of length $n$ is at distance no more than $t$ to exactly one codeword of $C$. 
linear perfect codes

Trivial perfect codes:
singletons; \{00 \cdots 0, 11 \cdots 1\} \quad (n \text{ odd})

Nontrivial linear perfect codes:
Hamming codes; Golay code \(G_{23}\); Golay code \(G_{11}\)

**Theorem**

(Tietäväinen-van Lint, Zinov’ev-Leont’ev, 1970s)
*These are the only nontrivial linear perfect codes.*

However, there are many nontrivial nonlinear perfect codes.
A code in a graph $\Gamma = (V, E)$ is a subset of $V$.

A code $C$ is a perfect $t$-code in $\Gamma$ if every vertex is at distance no more than $t$ to exactly one vertex of $C$.

That is, the $t$-neighbourhoods of the vertices of $C$ form a partition of $V$.

Perfect 1-codes = efficient dominating sets = independent perfect dominating sets

Perfect $t$-codes = perfect $t$-distance dominating sets
perfect codes in graphs

A code in a graph $\Gamma = (V, E)$ is a subset of $V$.

A code $C$ is a perfect $t$-code in $\Gamma$ if every vertex is at distance no more than $t$ to exactly one vertex of $C$.

That is, the $t$-neighbourhoods of the vertices of $C$ form a partition of $V$.

Perfect 1-codes = efficient dominating sets = independent perfect dominating sets

Perfect $t$-codes = perfect $t$-distance dominating sets
• A code in a graph $\Gamma = (V, E)$ is a subset of $V$.
• A code $C$ is a perfect $t$-code in $\Gamma$ if every vertex is at distance no more than $t$ to exactly one vertex of $C$.
• That is, the $t$-neighbourhoods of the vertices of $C$ form a partition of $V$.
• Perfect 1-codes = efficient dominating sets = independent perfect dominating sets
• Perfect $t$-codes = perfect $t$-distance dominating sets
A code in a graph $\Gamma = (V, E)$ is a subset of $V$.

A code $C$ is a perfect $t$-code in $\Gamma$ if every vertex is at distance no more than $t$ to exactly one vertex of $C$.

That is, the $t$-neighbourhoods of the vertices of $C$ form a partition of $V$.

Perfect 1-codes = efficient dominating sets = independent perfect dominating sets

Perfect $t$-codes = perfect $t$-distance dominating sets
A code in a graph $\Gamma = (V, E)$ is a subset of $V$.

A code $C$ is a perfect $t$-code in $\Gamma$ if every vertex is at distance no more than $t$ to exactly one vertex of $C$.

That is, the $t$-neighbourhoods of the vertices of $C$ form a partition of $V$.

Perfect 1-codes = efficient dominating sets = independent perfect dominating sets

Perfect $t$-codes = perfect $t$-distance dominating sets
perfect codes
perfect codes in Cayley graphs
cyclotomic graphs
circulant graphs
subgroups as perfect codes

a brief history

- N. Biggs (1973): distance-transitive graphs
- P. Delsarte (1973): association schemes (in particular, distance-regular graphs)
- J. Kratochvíl (1986): general graphs
- Many results in the literature
perfect codes

perfect codes in Cayley graphs
cyclotomic graphs
circulant graphs
subgroups as perfect codes

a brief history

- N. Biggs (1973): distance-transitive graphs
- P. Delsarte (1973): association schemes (in particular, distance-regular graphs)
  - J. Kratochvíl (1986): general graphs
- Many results in the literature
a brief history

- N. Biggs (1973): distance-transitive graphs
- P. Delsarte (1973): association schemes (in particular, distance-regular graphs)
- J. Kratochvíl (1986): general graphs
- Many results in the literature
motivation for studying perfect codes in Cayley graphs

- $q$-ary perfect $t$-codes of length $n = \text{perfect } t\text{-codes in Hamming graph } H(n, q)$
- $H(n, q)$ corresponds to an association scheme, leading to Biggs and Delsarte's work on perfect codes in distance-transitive graphs and association schemes.
- $H(n, q)$ can be also viewed as a Cayley graph.
- $q$-ary perfect $t$-codes of length $n$ w.r.t. the Lee metric are precisely perfect $t$-codes in $C_q \square \cdots \square C_q$ (which is also a Cayley graph)
motivation for studying perfect codes in Cayley graphs

- $q$-ary perfect $t$-codes of length $n = \text{perfect } t\text{-codes in Hamming graph } H(n, q)$
- $H(n, q)$ corresponds to an association scheme, leading to Biggs and Delsarte's work on perfect codes in distance-transitive graphs and association schemes.
- $H(n, q)$ can be also viewed as a Cayley graph.
- $q$-ary perfect $t$-codes of length $n$ w.r.t. the Lee metric are precisely perfect $t$-codes in $C_q \square \cdots \square C_q$ (which is also a Cayley graph)
motivation for studying perfect codes in Cayley graphs

• $q$-ary perfect $t$-codes of length $n = \text{perfect } t\text{-codes in Hamming graph } H(n, q)$

• $H(n, q)$ corresponds to an association scheme, leading to Biggs and Delsarte’s work on perfect codes in distance-transitive graphs and association schemes.

• $H(n, q)$ can be also viewed as a Cayley graph.

• $q$-ary perfect $t$-codes of length $n$ w.r.t. the Lee metric are precisely perfect $t$-codes in $C_q \square \cdots \square C_q$ (which is also a Cayley graph)
motivation for studying perfect codes in Cayley graphs

- $q$-ary perfect $t$-codes of length $n = \text{perfect } t\text{-codes in Hamming graph } H(n, q)$
- $H(n, q)$ corresponds to an association scheme, leading to Biggs and Delsarte's work on perfect codes in distance-transitive graphs and association schemes.
- $H(n, q)$ can be also viewed as a Cayley graph.
- $q$-ary perfect $t$-codes of length $n$ w.r.t. the Lee metric are precisely perfect $t$-codes in $C_q \square \cdots \square C_q$ (which is also a Cayley graph)
• A factorization of $G$ is a pair $(A, B)$ of subsets of $G$, not necessarily subgroups, such that every element of $G$ can be uniquely represented as $ab$ where $a \in A$ and $b \in B$.

• A tiling of $G$ is a normed factorization $(A, B)$ of $G$, in the sense that $e \in A \cap B$.

• If $(A, B)$ is a tiling of $G$ such that $A^{-1} = A$, then $B$ is a perfect code of $\text{Cay}(G, A \setminus \{e\})$. 
• A factorization of $G$ is a pair $(A, B)$ of subsets of $G$, not necessarily subgroups, such that every element of $G$ can be uniquely represented as $ab$ where $a \in A$ and $b \in B$.

• A tiling of $G$ is a normed factorization $(A, B)$ of $G$, in the sense that $e \in A \cap B$.

• If $(A, B)$ is a tiling of $G$ such that $A^{-1} = A$, then $B$ is a perfect code of $\text{Cay}(G, A \setminus \{e\})$. 
• A \textbf{factorization} of $G$ is a pair $(A, B)$ of subsets of $G$, not necessarily subgroups, such that every element of $G$ can be uniquely represented as $ab$ where $a \in A$ and $b \in B$.
• A \textbf{tiling} of $G$ is a \textbf{normed} factorization $(A, B)$ of $G$, in the sense that $e \in A \cap B$.
• If $(A, B)$ is a tiling of $G$ such that $A^{-1} = A$, then $B$ is a perfect code of $\text{Cay}(G, A \setminus \{e\})$. 
perfect codes in Cayley graphs

Problem
Construct/characterize/classify perfect $t$-codes in a given Cayley graph or prove that such a code does not exist.
perfect codes
perfect codes in Cayley graphs
cyclotomic graphs
circulant graphs
subgroups as perfect codes

a few known results

• Folklore: $-1$ must be an eigenvalue if a regular graph has a perfect 1-code
• G. Etienne (1987): necessary condition for the existence of perfect 1-codes in “normal” Cayley graphs
• J. Lee (2001): existence of perfect 1-codes in “normal” Cayley graphs in terms of covers of complete graphs
• I. J. Dejter and O. Serra (2003): E-chains of Cayley graphs on symmetric groups
• Special families such as circulants
a few known results

- Folklore: $-1$ must be an eigenvalue if a regular graph has a perfect 1-code
- G. Etienne (1987): necessary condition for the existence of perfect 1-codes in “normal” Cayley graphs
  - J. Lee (2001): existence of perfect 1-codes in “normal” Cayley graphs in terms of covers of complete graphs
  - I. J. Dejter and O. Serra (2003): E-chains of Cayley graphs on symmetric groups
- Special families such as circulants
A few known results

- Folklore: $-1$ must be an eigenvalue if a regular graph has a perfect 1-code.
- J. Lee (2001): existence of perfect 1-codes in “normal” Cayley graphs in terms of covers of complete graphs.
- Special families such as circulants.
a few known results

- Folklore: $-1$ must be an eigenvalue if a regular graph has a perfect 1-code
- G. Etienne (1987): necessary condition for the existence of perfect 1-codes in “normal” Cayley graphs
- J. Lee (2001): existence of perfect 1-codes in “normal” Cayley graphs in terms of covers of complete graphs
- I. J. Dejter and O. Serra (2003): E-chains of Cayley graphs on symmetric groups

- Special families such as circulants
a few known results

- Folklore: $-1$ must be an eigenvalue if a regular graph has a perfect 1-code
- G. Etienne (1987): necessary condition for the existence of perfect 1-codes in “normal” Cayley graphs
- J. Lee (2001): existence of perfect 1-codes in “normal” Cayley graphs in terms of covers of complete graphs
- I. J. Dejter and O. Serra (2003): E-chains of Cayley graphs on symmetric groups
- Special families such as circulants
Sufficient conditions for perfect codes in Gaussian and Eisenstein-Jacobi graphs were given by C. Martínez, et al. (2007-08)

Such conditions are also necessary (Zhou, 2015).

Gaussian and EJ graphs are two subfamilies of cyclotomic graphs.
cycloctomic graphs

- Sufficient conditions for perfect codes in Gaussian and Eisenstein-Jacobi graphs were given by C. Martínez, et al. (2007-08)
- Such conditions are also necessary (Zhou, 2015).
- Gaussian and EJ graphs are two subfamilies of cycloctomic graphs.
Sufficient conditions for perfect codes in Gaussian and Eisenstein-Jacobi graphs were given by C. Martínez, et al. (2007-08)

Such conditions are also necessary (Zhou, 2015).

Gaussian and EJ graphs are two subfamilies of cyclotomic graphs.
• Take an $m$th primitive root $\zeta_m$ of unity, e.g. $\zeta_m = e^{2\pi i / m}$, where $m \geq 3$.

• Let $A$ be a nonzero ideal of $\mathbb{Z}[\zeta_m]$.

• $G_m(A)$: Cayley graph of $\mathbb{Z}[\zeta_m]/A$ with connection set \{\(\pm (\zeta_m^i + A) : 0 \leq i \leq m - 1\}\).

• $G_m(A)$ is a finite, connected, arc-transitive graph with order $N(A)$ and valency a divisor of $2m$.

• $G_m^*(A)$: Cayley graphs of $\mathbb{Z}[\zeta_m]/A$ with connection set \{\(\pm (\zeta_m^i + A) : 0 \leq i \leq \phi(m) - 1\}\).

• $G_m^*(A)$ is a spanning subgraph of $G_m(A)$. 
• Take an \( m \)th primitive root \( \zeta_m \) of unity, e.g. \( \zeta_m = e^{2\pi i/m} \), where \( m \geq 3 \).

• Let \( A \) be a nonzero ideal of \( \mathbb{Z}[\zeta_m] \).

  • \( G_m(A) \): Cayley graph of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{\pm (\zeta_m^i + A) : 0 \leq i \leq m - 1 \} \).

  • \( G_m(A) \) is a finite, connected, arc-transitive graph with order \( N(A) \) and valency a divisor of \( 2m \).

  • \( G_m^*(A) \): Cayley graphs of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{\pm (\zeta_m^i + A) : 0 \leq i \leq \phi(m) - 1 \} \).

  • \( G_m^*(A) \) is a spanning subgraph of \( G_m(A) \).
• Take an \( m \)th primitive root \( \zeta_m \) of unity, e.g. \( \zeta_m = e^{2\pi i/m} \), where \( m \geq 3 \).

• Let \( A \) be a nonzero ideal of \( \mathbb{Z}[\zeta_m] \).

• \( G_m(A) \): Cayley graph of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{ \pm(\zeta_m^i + A) : 0 \leq i \leq m - 1 \} \).

• \( G_m(A) \) is a finite, connected, arc-transitive graph with order \( N(A) \) and valency a divisor of \( 2m \).

• \( G^*_m(A) \): Cayley graphs of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{ \pm(\zeta_m^i + A) : 0 \leq i \leq \phi(m) - 1 \} \).

• \( G^*_m(A) \) is a spanning subgraph of \( G_m(A) \).
• Take an \( m \)th primitive root \( \zeta_m \) of unity, e.g. \( \zeta_m = e^{2\pi i / m} \), where \( m \geq 3 \).

• Let \( A \) be a nonzero ideal of \( \mathbb{Z}[\zeta_m] \).

• \( G_m(A) \): Cayley graph of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{ \pm (\zeta_m^i + A) : 0 \leq i \leq m - 1 \} \).

• \( G_m(A) \) is a finite, connected, arc-transitive graph with order \( N(A) \) and valency a divisor of \( 2m \).

• \( G^*_m(A) \): Cayley graphs of \( \mathbb{Z}[\zeta_m]/A \) with connection set \( \{ \pm (\zeta_m^i + A) : 0 \leq i \leq \phi(m) - 1 \} \).

• \( G^*_m(A) \) is a spanning subgraph of \( G_m(A) \).
• Take an $m$th primitive root $\zeta_m$ of unity, e.g. $\zeta_m = e^{2\pi i / m}$, where $m \geq 3$.

• Let $A$ be a nonzero ideal of $\mathbb{Z}[\zeta_m]$.

• $G_m(A)$: Cayley graph of $\mathbb{Z}[\zeta_m]/A$ with connection set $\{\pm(\zeta_i^j + A) : 0 \leq i \leq m - 1\}$.

• $G_m(A)$ is a finite, connected, arc-transitive graph with order $N(A)$ and valency a divisor of $2m$.

• $G^*_m(A)$: Cayley graphs of $\mathbb{Z}[\zeta_m]/A$ with connection set $\{\pm(\zeta_i^j + A) : 0 \leq i \leq \phi(m) - 1\}$.

• $G^*_m(A)$ is a spanning subgraph of $G_m(A)$. 
• Take an $m$th primitive root $\zeta_m$ of unity, e.g. $\zeta_m = e^{2\pi i / m}$, where $m \geq 3$.

• Let $A$ be a nonzero ideal of $\mathbb{Z}[\zeta_m]$.

• $G_m(A)$: Cayley graph of $\mathbb{Z}[\zeta_m]/A$ with connection set $\{\pm (\zeta_m^i + A) : 0 \leq i \leq m - 1\}$.

• $G_m(A)$ is a finite, connected, arc-transitive graph with order $N(A)$ and valency a divisor of $2m$.

• $G^*_m(A)$: Cayley graphs of $\mathbb{Z}[\zeta_m]/A$ with connection set $\{\pm (\zeta_m^i + A) : 0 \leq i \leq \phi(m) - 1\}$.

• $G^*_m(A)$ is a spanning subgraph of $G_m(A)$. 
Distance in $G_m^*(A)$ is the Mannheim distance, but distance in $G_m(A)$ is not well understood.

Denote $\bar{\alpha} = \alpha + A$ for $\alpha \in \mathbb{Z}[\zeta_m]$.

The distance between $\bar{\alpha}$ and $\bar{\beta}$ in $G_m^*(A)$ is the Mannheim distance

$$\|\bar{\alpha} - \bar{\beta}\|,$$

where

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\},$$

where

$$|\alpha| := \sum_{i=0}^{\phi(m)-1} |a_i|$$

for

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m].$$
Distance in $G_m^*(A)$ is the Mannheim distance, but distance in $G_m(A)$ is not well understood.

Denote $\bar{\alpha} = \alpha + A$ for $\alpha \in \mathbb{Z}[\zeta_m]$.

The distance between $\bar{\alpha}$ and $\bar{\beta}$ in $G_m^*(A)$ is the Mannheim distance

$$\|\bar{\alpha} - \bar{\beta}\|,$$

where

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\},$$

where

$$|\alpha| := \sum_{i=0}^{\phi(m)-1} |a_i|$$

for

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m].$$
Distance in $G^*_m(A)$ is the Mannheim distance, but distance in $G_m(A)$ is not well understood.

Denote $\bar{\alpha} = \alpha + A$ for $\alpha \in \mathbb{Z}[\zeta_m]$.

The distance between $\bar{\alpha}$ and $\bar{\beta}$ in $G^*_m(A)$ is the Mannheim distance

$$\|\bar{\alpha} - \bar{\beta}\|,$$

where

$$\|\bar{\alpha}\| := \min\{|\alpha - \delta| : \delta \in A\},$$

where

$$|\alpha| := \sum_{i=0}^{\phi(m)-1} |a_i|$$

for

$$\alpha = \sum_{i=0}^{\phi(m)-1} a_i \zeta_m^i \in \mathbb{Z}[\zeta_m].$$
Let $D$ be an ideal of $\mathbb{Z}[\zeta_m]$ containing $A$.

**Lemma**

(a) $D/A$ is a perfect $t$-code in $G_m^*(A)$ iff

$$\text{norm of } D = \text{size of the } t\text{-neighbourhood of any vertex}$$

and for any $\delta \in A$ and $\eta \in D - A$,

$$|\eta - \delta| \geq 2t + 1. \quad (1)$$

(b) $D/A$ is a perfect $t$-code in $G_m(A)$ only if

$$\text{norm of } D = \text{size of the } t\text{-neighbourhood of any vertex}$$

and (1) holds.
Let $D$ be an ideal of $\mathbb{Z}[\zeta_m]$ containing $A$.

**Lemma**

(a) $D/A$ is a perfect $t$-code in $G^*_m(A)$ iff

\[ \text{norm of } D = \text{size of the } t\text{-neighbourhood of any vertex} \]

and for any $\delta \in A$ and $\eta \in D - A,$

\[ |\eta - \delta| \geq 2t + 1. \]  \hspace{1cm} (1)

(b) $D/A$ is a perfect $t$-code in $G_m(A)$ only if

\[ \text{norm of } D = \text{size of the } t\text{-neighbourhood of any vertex} \]

and (1) holds.
m = 4: Gaussian graphs

Example

(C. Martínez, et al. 2007)
Take $\zeta_4 = i$, $i^2 = -1$. Then

$$\mathbb{Z}[i] = \{x + yi : x, y \in \mathbb{Z}\}$$

is the ring of Gaussian integers, with norm

$$N(x + yi) = x^2 + y^2.$$ 

Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ be such that $N(\alpha) \geq 5$. Call

$$G_\alpha := G_4((\alpha)) = G_4^*((\alpha))$$

a Gaussian network.
perfect codes in Gaussian graphs

**Theorem**

Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ ($a, b \geq 0$) and $0 \neq \beta \in \mathbb{Z}[i]$ be such that $N(\alpha) \geq 5$ and $\beta$ divides $\alpha$.

Let $t$ be an integer between $1$ and $\lfloor (a + b - 1)/2 \rfloor$.

Then $(\beta)/(\alpha)$ is a perfect $t$-code in $G_\alpha$ if and only if $\beta$ is an associate of $t + (t + 1)i$ or $t - (t + 1)i$.

[S. Zhou, 2015]
Theorem

Let $0 \neq \alpha = a + bi \in \mathbb{Z}[i]$ $(a, b \geq 0)$ and $0 \neq \beta \in \mathbb{Z}[i]$ be such that $N(\alpha) \geq 5$ and $\beta$ divides $\alpha$.

Let $t$ be an integer between $1$ and $\lfloor (a + b - 1)/2 \rfloor$.

Then $(\beta)/(\alpha)$ is a perfect $t$-code in $G_\alpha$ if and only if $\beta$ is an associate of $t + (t + 1)i$ or $t - (t + 1)i$.

[S. Zhou, 2015]
**$m = 3$: Eisenstein-Jacobi graphs**

**Example**

(C. Martínez, et al. 2007)
Take $\zeta_3 = -\rho := -(1 + \sqrt{-3})/2$. Then

$$\mathbb{Z}[\rho] = \{ c + d\rho : c, d \in \mathbb{Z} \}$$

is the ring of Eisenstein-Jacobi integers, with norm

$$N(x + y\rho) = x^2 + xy + y^2.$$  

Call

$$EJ_\alpha := G_3((\alpha))$$

an Eisenstein-Jacobi (EJ) graph.
perfect codes in EJ graphs

**Theorem**

Let $0 \neq \alpha = a + b\rho \in \mathbb{Z}[\rho]$ $(a, b \geq 0)$ and $0 \neq \beta \in \mathbb{Z}[\rho]$ be such that $N(\alpha) \geq 7$ and $\beta$ divides $\alpha$.

Let $t$ be an integer between $1$ and $\lfloor (a + b - 1)/2 \rfloor$.

Then $(\beta)/(\alpha)$ is a perfect $t$-code in $EJ_\alpha$ if and only if $\beta$ is an associate of $(t + 1) + t\rho$ or $t + (t + 1)\rho$.


[S. Zhou, 2015]
perfect codes in EJ graphs

Theorem

Let $0 \neq \alpha = a + b \rho \in \mathbb{Z}[\rho]$ ($a, b \geq 0$) and $0 \neq \beta \in \mathbb{Z}[\rho]$ be such that $N(\alpha) \geq 7$ and $\beta$ divides $\alpha$.

Let $t$ be an integer between 1 and $\lfloor (a + b - 1)/2 \rfloor$.

Then $(\beta)/(\alpha)$ is a perfect $t$-code in $EJ_\alpha$ if and only if $\beta$ is an associate of $(t + 1) + t \rho$ or $t + (t + 1) \rho$.

[S. Zhou, 2015]
Example

\[ EJ_{1+9\rho} \cong \text{Cay}(\mathbb{Z}_{91}, \{\pm 10, \pm 9, \pm 1\}) \]
\[ f : x + y\rho \mod (1 + 9\rho) \mapsto x + 10y \mod 91. \]

The only perfect code in \( EJ_{1+9\rho} \) of the form \( \beta/(1 + 9\rho) \) is

\( (2 + \rho)/(1 + 9\rho), \)

which is a perfect 1-code with size \( N(1 + 9\rho)/N(2 + \rho) = 13. \)
Example

\[ E_{J_{1+9\rho}} \cong \text{Cay}(\mathbb{Z}_{91}, \{\pm 10, \pm 9, \pm 1\}) \]

\[ f : x + y\rho \mod (1 + 9\rho) \mapsto x + 10y \mod 91. \]

The only perfect code in \( E_{J_{1+9\rho}} \) of the form \((\beta)/(1 + 9\rho)\) is

\[ (2 + \rho)/(1 + 9\rho), \]

which is a perfect 1-code with size \( N(1 + 9\rho)/N(2 + \rho) = 13. \)
We have

\[(2 + \rho)/(1 + 9\rho) = \{j(1 + 2\rho) \mod (1 + 9\rho) : 0 \leq j \leq 12\}\].

Since

\[f : j(1 + 2\rho) \mod (1 + 9\rho) \mapsto 21j \mod 91, \ 0 \leq j \leq 12,\]

we may view \((2 + \rho)/(1 + 9\rho)\) as the perfect 1-code

\[C = \{0, 21, 42, 63, 84, 14, 35, 56, 77, 7, 28, 49, 70\} \mod 91\]

in \(\text{Cay}(\mathbb{Z}_{91}, \{\pm 10, \pm 9, \pm 1\})\).
A perfect 1-code in $EJ_{1+9\rho} \cong \text{Cay}(\mathbb{Z}_{91}, \{\pm 10, \pm 9, \pm 1\})$
Example
Let $p$ be an odd prime and $n \geq 2p + 1$ an integer with $n \equiv 1 \mod 2p$.

Then every $2p$-valent first kind Frobenius circulant is isomorphic to a cyclotomic graph $G_p(A)$ for some ideal $A$ of $\mathbb{Z}[\zeta_p]$. 
perfecst codes in circulants

- N. Obradović, et al. (2007): if $|S| = 3$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff $n \equiv 4 \mod 8$; if $|S| = 4$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod 5.

- Y-P. Deng (2014): necessary and sufficient condition for a circulant graph to admit a perfect code with size a prime number.

- K. Reji Kumar and G. MacGillivray (2013): a few results on perfect codes in circulant graphs.
perfects codes in circulants

- N. Obradović, et al. (2007): if $|S| = 3$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff $n \equiv 4 \mod 8$;
  if $|S| = 4$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod 5.
- Y-P. Deng (2014): necessary and sufficient condition for a circulant graph to admit a perfect code with size a prime number.
- K. Reji Kumar and G. MacGillivray (2013): a few results on perfect codes in circulant graphs.
perfects codes in circulants

- N. Obradović, et al. (2007): 
  if $|S| = 3$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff $n \equiv 4 \mod 8$;  
  if $|S| = 4$, then $\text{Cay}(\mathbb{Z}_n, S)$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod 5.

- Y-P. Deng (2014): necessary and sufficient condition for a circulant graph to admit a perfect code with size a prime number.

- K. Reji Kumar and G. MacGillivray (2013): a few results on perfect codes in circulant graphs.
Theorem
(Feng, Huang and Z, 2017)
Let $p$ be an odd prime.
A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p - 1$ admits a perfect code iff $p$ divides $n$ and the elements of $S \cup \{0\}$ are pairwise distinct mod $p$.

Theorem
(Feng, Huang and Z, 2017)
Let $p$ be a prime and $l$ the exponent of $p$ in $n$.
A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p^l - 1$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod $p^l$.

Y-P. Deng et al. (2017): Similar results but different approach. They also considered valency $pq$ coprime to $n/pq$. 
Theorem
(Feng, Huang and Z, 2017)
Let $p$ be an odd prime.
A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p - 1$ admits a perfect code iff $p$ divides $n$ and the elements of $S \cup \{0\}$ are pairwise distinct mod $p$.

Theorem
(Feng, Huang and Z, 2017)
Let $p$ be a prime and $l$ the exponent of $p$ in $n$.
A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p^l - 1$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod $p^l$.

Y-P. Deng et al. (2017): Similar results but different approach. They also considered valency $pq$ coprime to $n/pq$. 
Theorem
(Feng, Huang and Z, 2017)
Let $p$ be an odd prime.

A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p - 1$ admits a perfect code iff $p$ divides $n$ and the elements of $S \cup \{0\}$ are pairwise distinct mod $p$.

Theorem
(Feng, Huang and Z, 2017)
Let $p$ be a prime and $l$ the exponent of $p$ in $n$.

A connected circulant graph $\text{Cay}(\mathbb{Z}_n, S)$ of valency $p^l - 1$ admits a perfect code iff the elements of $S \cup \{0\}$ are pairwise distinct mod $p^l$.

Y-P. Deng et al. (2017): Similar results but different approach. They also considered valency $pq$ coprime to $n/pq$. 
normal subgroups as perfect codes

**Definition**
A subset $C$ of a group $G$ is called a perfect 1-code of $G$ if it is a perfect 1-code in some Cayley graph of $G$.

**Theorem**
(Huang, Xia and Z, 2017+)
Let $G$ be a group and $H$ a normal subgroup of $G$. Then $H$ is a perfect 1-code of $G$ iff

$$\forall g \in G \ (g^2 \in H) \ \exists h \in H \ ((gh)^2 = e).$$

**Corollary**
Any normal subgroup with odd order or odd index is a perfect code.
In particular, any normal subgroup of a group of odd order is a perfect code.
normal subgroups as perfect codes

Definition
A subset $C$ of a group $G$ is called a perfect 1-code of $G$ if it is a perfect 1-code in some Cayley graph of $G$.

Theorem
(Huang, Xia and Z, 2017+)
Let $G$ be a group and $H$ a normal subgroup of $G$. Then $H$ is a perfect 1-code of $G$ iff

$$\forall g \in G \ (g^2 \in H) \ \exists h \in H \ ((gh)^2 = e).$$

Corollary
Any normal subgroup with odd order or odd index is a perfect code.
In particular, any normal subgroup of a group of odd order is a perfect code.
normal subgroups as perfect codes

Definition
A subset $C$ of a group $G$ is called a perfect 1-code of $G$ if it is a perfect 1-code in some Cayley graph of $G$.

Theorem
(Huang, Xia and Z, 2017+)
Let $G$ be a group and $H$ a normal subgroup of $G$. Then $H$ is a perfect 1-code of $G$ iff

$$\forall g \in G \ (g^2 \in H) \ \exists h \in H \ ((gh)^2 = e).$$

Corollary
Any normal subgroup with odd order or odd index is a perfect code.
In particular, any normal subgroup of a group of odd order is a perfect code.
Theorem
(Huang, Xia and Z, 2017+)
Let $G$ be an abelian group with Sylow 2-subgroup $P = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$.
Suppose that $H$ is a subgroup of $G$ such that $H \cap P$ is cyclic.
Then $H$ is a perfect code of $G$ iff either $H \cap P$ is trivial or $H \cap P$ projects onto at least one of $\langle a_1 \rangle, \ldots, \langle a_n \rangle$.

Corollary
(Huang, Xia and Z, 2017+)
Let $G$ be a cyclic group and $H$ a subgroup of $G$.
Then $H$ is a perfect code of $G$ iff either $|H|$ or $|G/H|$ is odd.
Theorem

(Huang, Xia and Z, 2017+)
Let $G$ be an abelian group with Sylow 2-subgroup $P = \langle a_1 \rangle \times \cdots \times \langle a_n \rangle$.
Suppose that $H$ is a subgroup of $G$ such that $H \cap P$ is cyclic.
Then $H$ is a perfect code of $G$ iff either $H \cap P$ is trivial or $H \cap P$ projects onto at least one of $\langle a_1 \rangle, \ldots, \langle a_n \rangle$.

Corollary

(Huang, Xia and Z, 2017+)
Let $G$ be a cyclic group and $H$ a subgroup of $G$.
Then $H$ is a perfect code of $G$ iff either $\vert H \vert$ or $\vert G/H \vert$ is odd.
**Theorem**

*(Huang, Xia and Z, 2017+)*

Let \( D_{2n} = \langle a, b \mid a^n = b^2 = (ab)^2 = e \rangle \), and let \( H \) be a proper subgroup of \( D_{2n} \).

Then \( H \) is a perfect code of \( D_{2n} \) iff either \( H \not\subseteq \langle a \rangle \), or \( H \leq \langle a \rangle \) and at least one of \(|H|\) and \( n/|H| \) is odd.