Simple construction of \([2^k - 1 + k, k, 2^{k-1} + 1]\) codes attaining the Griesmer bound

Jeong-Heon Kim and Hong-Yeop Song
Yonsei University
Griesmer bound

• Description follows
Griesmer bound

• For any \([n,k,d]\) code,

\[
n \geq \sum_{i=0}^{k-1} \left\lfloor d / 2^i \right\rfloor
\]

• An \([n,k,d]\) code with the equality is said to be optimal
Brief history

• For \( d \leq 2^{k-1} \)
  – In 1965, Solomon and Stiffler
  – In 1974, Belov
  – In 1981, Helleseth

• For \( d > 2^{k-1} \)
  – In 1981, Helleseth and van Tilborg
  – In 1983, Helleseth
A new construction

Let’s consider a code $C$ with the following generator matrix:

$$G = \begin{bmatrix} P_{2^k - 1} & I_k \end{bmatrix}$$

Then, $C$ is a code and attains the Griesmer bound.
Proof (1)

- The minimum distance of \( C \) is \( 2^{k-1} + 1 \)
  - for any \( c \in C, c \neq 0 \)
    \[
    c = (h | m)
    \]

where \( h \) is some codeword of the dual code of the \([2^k - l, 2^k - l - k]\) Hamming code and \( m \) is a message vector.
Proof (2)

• C attains the Griesmer bound