Advances in Applied Mathematics 应用数学进展, 2021, 10(2), 575-586
Published Online February 2021 in Hans. http://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2021.102063

Hans汉斯

一种基于有限域的二进制和多进制空间耦合LDPC码构造方法

梁　宇，杨卫华*，李玉瑛

太原理工大学数学学院，山西　晋中
Email: 838606385@qq.com, *yangweihua@tyut.edu.cn, 13803491408@163.com

收稿日期：2021年1月23日；录用日期：2021年2月17日；发布日期：2021年2月26日

摘　要

空间耦合LDPC (Spatially-Coupled LDPC, SC-LDPC)码由于阈值饱和特性，被证明是未来无线通信系统的有力候选码型。SC-LDPC码是一种卷积LDPC码，在二元无记忆对称信道下采用置信传播算法时具有逼近香农限的性能。本文提出了一种构造二进制和多进制空间耦合LDPC码的统一方法。基于有限域$GF(q)$上的本原元、加法子群、乘法子群，构造了6类二进制和多进制空间耦合准循环LDPC码(Spatially-Coupled Quasi- Cyclic LDPC, SC-QC-LDPC)，用此构造的LDPC码的围长至少为6。

关键词

空间耦合LDPC码，准循环LDPC码，有限域，围长

An Approach for Constructing Binary and Nonbinary Spatially-Coupled LDPC Codes Based on Finite Fields

Yu Liang, Weihua Yang*, Yuying Li

School of Mathematics, Taiyuan University of Technology, Jinzhong Shanxi
Email: 838606385@qq.com, *yangweihua@tyut.edu.cn, 13803491408@163.com

Received: Jan. 23rd, 2021; accepted: Feb. 17th, 2021; published: Feb. 26th, 2021

Abstract

Spatially-coupled LDPC codes are demonstrated to strong candidates for future optical communications systems due to the threshold saturating property. Spatially-coupled LDPC code is a kind of convolutional LDPC code. It has the performance of approaching Shannon limit when using belief propagation decoding algorithm in binary memoryless symmetric channel. A unified approach for

文章引用: 梁宇, 杨卫华, 李玉瑛. 一种基于有限域的二进制和多进制空间耦合 LDPC 码构造方法[J]. 应用数学进展, 2021, 10(2): 575-586. DOI: 10.12677/aam.2021.102063

constructing binary and nonbinary spatially-coupled LDPC codes is presented in this paper. Six classes of binary and nonbinary spatially-coupled Quasi-Cyclic LDPC codes are constructed based on primitive elements, additive subgroups, multiplicative subgroups of finite fields. Moreover, the girth of these codes is greater than or equal to 6.

Keywords

Spatially-Coupled LDPC Codes, Quasi-Cyclic LDPC Codes, Finite Field, Girth

1. 引言

空间耦合 LDPC 码源自于 LDPC 卷积码[1]，由于其优良的阈值而受到人们的广泛关注。对于二元无记忆对称(Binary memoryless symmetric, BMS)信道，已经证明了规则 LDPC 码集[2]的最大后验概率(Maximum aposteriori probability, MAP)阈值可以通过空间耦合原始 LDPC 码集的生成码集的置信传播(Belief propagation, BP)阈值来逼近[3] [4] [5] [6]，这就是所谓的阈值饱和现象。除了渐近性能分析外，SC-LDPC 码的有限长性能特别是利用窗口译码方法进行译码，也成为研究的重点[7] [8]。最近，多进制 SC-LDPC 码也开始受到研究人员的关注。多进制 SC-LDPC 码的阈值饱和现象在二元删除信道(Binary erasure channel, BEC)被研究[9]。经典的 SC-LDPC 码构造，被分类为图覆盖结构，是基于展开 LDPC 码的校验矩阵来形成 SC-LDPC 码的校验矩阵[1] [10]。

准循环 LDPC 码[11]由于其低复杂度和高度并行的编码[12]和译码[13]，已被各种通信系统标准化，最近又应用于数据存储产品中。QC-LDPC 码通常是由在有限域上相同大小的稀疏循环矩阵的阵列的零空间给出的[15]。QC-LDPC 码具有优良有限长性能和高效硬件实现的优点[12] [13] [14]。广泛的仿真结果[15] [16] [17]已经表明设计良好的 QC-LDPC 码优于非结构化随机 LDPC 码。仿真结果还表明，非二进制原模图 LDPC 码的性能优于与其对应的二进制码[18]。

由于 QC-LDPC 码和 SC-LDPC 码的优点，本文从理论上研究了在任意有限域上具有准循环结构的 SC-LDPC 码的构造，此类码称之为 SC-QC-LDPC 码。最近，二进制 SC-QC-LDPC 码的构造[19]使用了一种改进的渐进边缘增长(Progressive edge growth, PEG)算法[20]。相反，本文构造 SC-QC-LDPC 码是基于有限域的确定性构造。这避免了耗时的计算机搜索，同时确保了校验矩阵的 Tanner 图的围长至少为 6，这也通常保证了码的优良性能。

2. 预备知识

2.1. 有限域中元素的位置向量

考虑有限域 $GF(q)$，q 为一个素数的幂。令 α 为 $GF(q)$ 的本原元，则 α 的 q 个幂次 $\alpha^{-\infty}=0$，$\alpha^0=1$，$\alpha,\cdots,\alpha^{q-2}$ 表示出了 $GF(q)$ 的所有元素，且 $\alpha^{q-1}=1$。$GF(q)$ 包含两个群：加法群和乘法群。$GF(q)$ 的 q 个元素在加法运算下构成加法群，$GF(q)$ 的 $q-1$ 个非零元素在乘法运算下构成乘法群。

对于任意一个非零元素 α^i，$0\le i<q-1$，我们定义一个 $GF(2)$ 上的 $q-1$ 维向量：$z_b(\alpha^i)=(z_0,z_1,\cdots,z_{q-2})$，其中第 i 个分量 $z_i=1$，而其他 $q-2$ 个分量等于零。将这样只有一个 1 分量的 $GF(2)$ 上的 $q-1$ 维向量称为元素 α^i 的二进制位置向量(binary location-vector)。显然，域 $GF(q)$ 中两个不同非零元素的二进制位置向量的 1 分

量在不同位置上。元素 0 的二进制位置向量定义为$q-1$维全零向量$z_b(0)=(0,0,\cdots,0)$。类似地，对于任意一个非零元素α^i，$0\le i<q-1$，我们定义一个$GF(q)$上的$q-1$维向量$z_q(\alpha^i)=(z_0,z_1,\cdots,z_{q-2})$，其中第$i$个分量$z_i=\alpha^i$，而其他$q-2$个分量等于零。将这样只有一个$\alpha^i$分量的$GF(q)$上的$q-1$维向量称为元素$\alpha^i$的$q$进制位置向量($q$-ary location-vector)。元素 0 的q进制位置向量定义为$q-1$维全零向量$z_q(0)=(0,0,\cdots,0)$。

2.2. 有限域中元素的矩阵散列

令δ为$GF(q)$的一个非零元素。当$0\le i<q-1$时，$\alpha^i\delta$的二进制位置向量$z_b(\alpha^i\delta)$是$\alpha^{i-1}\delta$的二进制位置向量$z_b(\alpha^{i-1}\delta)$的循环移位(右移一位)。因为$\alpha^{q-1}=1$，则$z_b(\alpha^{q-1}\delta)=z_b(\delta)$。因而，$z_b(\delta)$就是$z_b(\alpha^{q-2}\delta)$的循环移位。以元素$\delta,\alpha\delta,\cdots,\alpha^{q-2}\delta$的二进制位置向量作为行，可以得到一个$GF(2)$上的$(q-1)\times(q-1)$矩阵$A_b(\delta)$。该矩阵是一个循环置换矩阵(Circulant permutation matrix, CPM)，其每一行都是上一行的循环移位，而第一行是最后一行的循环移位。将矩阵$A_b(\delta)$称为元素δ在$GF(2)$上的$(q-1)$重二进制矩阵散列((q-1)-fold binary matrix dispersion)。类似地，我们以元素$\delta,\alpha\delta,\cdots,\alpha^{q-2}\delta$的$q$进制位置向量作为行，可以得到一个$GF(q)$上的$(q-1)\times(q-1)$矩阵$A_q(\delta)$。该矩阵是一个$q$进制$\alpha$倍循环置换矩阵($q$-ary α-multiplied circulant permutation matrix)，其每一行都是上一行乘以α的循环移位，而第一行是最后一行乘以α的循环移位。将矩阵$A_q(\delta)$称为元素δ在$GF(q)$上的$(q-1)$重q进制矩阵散列((q-1)-fold q-ary matrix dispersion)。

3. 基于有限域构造 QC-LDPC 码的一般方法

令α为$GF(q)$的本原元。构造过程始于一个$GF(q)$上的$m\times n$矩阵

$$B=\begin{bmatrix}b_0\\b_1\\\vdots\\b_{m-1}\end{bmatrix}=\begin{bmatrix}b_{0,0}&b_{0,1}&\cdots&b_{0,n-1}\\b_{1,0}&b_{1,1}&\cdots&b_{1,n-1}\\\vdots&\vdots&\ddots&\vdots\\b_{m-1,0}&b_{m-1,1}&\cdots&b_{m-1,n-1}\end{bmatrix}$$

其行满足如下两个约束条件：1) 若$0\le i<m$，$0\le k,l<q-1$，且$k\ne l$，则$\alpha^k b_i$与$\alpha^l b_i$至多有一个对应位置上的值相同(即它们至少有$n-1$个对应位置上的值不同)；2) 若$0\le i,j<m$，$i\ne j$，且$0\le k,l<q-1$，则$\alpha^k b_i$与$\alpha^l b_j$至少有$n-1$个对应位置上的值不同。矩阵B的两个约束条件分别称为α乘行约束 1 和 2 (α-multiplied row constraint 1 and 2)。

定理 1：如果矩阵B的每一行至多有一个 0 元素且矩阵B的任意一个2×2子矩阵是非奇异的，则矩阵B满足α乘行约束 1 和 2。

证明：因为当且仅当$b_{i,s}=0$时，$\alpha^k b_{i,s}=\alpha^l b_{i,s}$，其中$0\le i<m$，$0\le k,l<q-1$，且$k\ne l$，所以当且仅当矩阵$B$的每一行至多有一个 0 元素，矩阵$B$满足$\alpha$乘行约束 1。假设矩阵$B$不满足$\alpha$乘行约束 2，则$\alpha^k b_{i,s}=\alpha^l b_{j,s}$，$\alpha^k b_{i,t}=\alpha^l b_{j,t}$，其中$0\le i,j<m$且$i\ne j$，$0\le k,l<q-1$，$0\le s,t<n$且$s\ne t$。因此$\alpha^k b_{i,s}\cdot\alpha^l b_{j,t}=\alpha^l b_{j,s}\cdot\alpha^k b_{i,t}$，由此推得$b_{i,s}\cdot b_{j,t}-b_{i,t}\cdot b_{j,s}=0$即矩阵$B$存在$2\times2$奇异子矩阵，矛盾。

定理 2：如果矩阵B满足α乘行约束 1 和 2，则矩阵B满足2×2子矩阵约束，即矩阵B中任意2×2子矩阵至少有一个 0 元素或是非奇异的。

证明：如果B满足α乘行约束 1 和 2，则$\alpha^k b_{i,s}=\alpha^l b_{i,s}$或$\alpha^k b_{i,s}\ne\alpha^l b_{i,s}$且$\alpha^k b_{i,s}=\alpha^l b_{j,s}$或$\alpha^k b_{i,s}\ne\alpha^l b_{j,s}$，其中$0\le i,j<m$且$i\ne j$，$0\le k,l<q-1$，$0\le s,t<n$且$s\ne t$。

情况 1：当$\alpha^k b_{i,s}=\alpha^l b_{i,s}$且$\alpha^k b_{i,s}=\alpha^l b_{j,s}$时，因为$\alpha^k b_{i,s}=\alpha^l b_{i,s}$，所以$b_{i,s}=0$；又因为$\alpha^k b_{i,s}=\alpha^l b_{j,s}$，所以$b_{j,s}=b_{i,s}=0$。因此$B_{2\times2}=\begin{bmatrix}b_{i,s}&b_{i,t}\\b_{j,s}&b_{j,t}\end{bmatrix}=\begin{bmatrix}0&b_{i,t}\\0&b_{j,t}\end{bmatrix}$，故$B$满足$2\times2$子矩阵约束。

情况 2：当 $\alpha^k b_{i,s}=\alpha^l b_{i,s}$ 且 $\alpha^k b_{i,s}\neq\alpha^l b_{j,s}$ 时，因为 $\alpha^k b_{i,s}=\alpha^l b_{i,s}$，所以 $b_{i,s}=0$；又因为 $\alpha^k b_{i,s}\neq\alpha^l b_{j,s}$，所以 $b_{j,s}\neq 0$。因此 $B_{2\times 2}=\begin{bmatrix} b_{i,s} & b_{i,t} \\ b_{j,s} & b_{j,t} \end{bmatrix}=\begin{bmatrix} 0 & b_{i,t} \\ b_{j,s} & b_{j,t} \end{bmatrix}$，$\det\left(B_{2\times 2}\right)=-b_{i,t}b_{j,s}\neq 0$，故 B 满足 2×2 子矩阵约束。

情况 3：当 $\alpha^k b_{i,s}\neq\alpha^l b_{i,s}$ 且 $\alpha^k b_{i,s}=\alpha^l b_{j,s}$ 时，因为 $\alpha^k b_{i,s}=\alpha^l b_{i,s}$ 且 $\alpha^k b_{i,s}=\alpha^l b_{j,s}$，所以 $\alpha^k b_{i,s}\alpha^l b_{j,t}\neq\alpha^k b_{i,t}\alpha^l b_{j,s}$，即 $b_{i,s}b_{j,t}\neq b_{i,t}b_{j,s}$。因此 $B_{2\times 2}=\begin{bmatrix} b_{i,s} & b_{i,t} \\ b_{j,s} & b_{j,t} \end{bmatrix}$，$\det\left(B_{2\times 2}\right)=b_{i,s}b_{j,t}-b_{i,t}b_{j,s}\neq 0$，故 B 满足 2×2 子矩阵约束。

情况 4：当 $\alpha^k b_{i,s}\neq\alpha^l b_{i,s}$ 且 $\alpha^k b_{i,s}\neq\alpha^l b_{j,s}$ 时，因为 $\alpha^k b_{i,s}\neq\alpha^l b_{i,s}$ 且 $\alpha^k b_{i,s}\neq\alpha^l b_{j,s}$，所以 $\alpha^k b_{i,s}\alpha^l b_{j,t}\neq\alpha^k b_{i,t}\alpha^l b_{j,s}$，即 $b_{i,s}b_{j,t}\neq b_{i,t}b_{j,s}$。因此 $B_{2\times 2}=\begin{bmatrix} b_{i,s} & b_{i,t} \\ b_{j,s} & b_{j,t} \end{bmatrix}$，$\det\left(B_{2\times 2}\right)=b_{i,s}b_{j,t}-b_{i,t}b_{j,s}\neq 0$，故 B 满足 2×2 子矩阵约束。

因此如果矩阵 B 满足 α 乘行约束 1 和 2，则矩阵 B 满足 2×2 子矩阵约束。

将矩阵 B 的每一项 $b_{i,j}$ 用其相应的 $(q-1)$ 重二进制矩阵散列 $A_b\left(b_{i,j}\right)$ 替换后，可以得到一个 $m\times n$ 阵列 H_b：

$$H_b=\begin{bmatrix} A_b\left(b_{0,0}\right) & A_b\left(b_{0,1}\right) & \cdots & A_b\left(b_{0,n-1}\right) \\ A_b\left(b_{1,0}\right) & A_b\left(b_{1,1}\right) & \cdots & A_b\left(b_{1,n-1}\right) \\ \vdots & \vdots & \ddots & \vdots \\ A_b\left(b_{m-1,0}\right) & A_b\left(b_{m-1,1}\right) & \cdots & A_b\left(b_{m-1,n-1}\right) \end{bmatrix}$$

其中，若 $b_{i,j}\neq 0$，则 $A_b\left(b_{i,j}\right)$ 是 $GF(2)$ 上的一个 $(q-1)\times(q-1)$ CPM；若 $b_{i,j}=0$，则 $A_b\left(b_{i,j}\right)$ 是一个全零矩阵。H_b 是 $GF(2)$ 上的一个 $m(q-1)\times n(q-1)$ 矩阵。

类似地，将矩阵 B 的每一项 $b_{i,j}$ 用其相应的 $(q-1)$ 重 q 进制矩阵散列 $A_q\left(b_{i,j}\right)$ 替换后，可以得到一个 $m\times n$ 阵列 H_q：

$$H_q=\begin{bmatrix} A_q\left(b_{0,0}\right) & A_q\left(b_{0,1}\right) & \cdots & A_q\left(b_{0,n-1}\right) \\ A_q\left(b_{1,0}\right) & A_q\left(b_{1,1}\right) & \cdots & A_q\left(b_{1,n-1}\right) \\ \vdots & \vdots & \ddots & \vdots \\ A_q\left(b_{m-1,0}\right) & A_q\left(b_{m-1,1}\right) & \cdots & A_q\left(b_{m-1,n-1}\right) \end{bmatrix}$$

其中，若 $b_{i,j}\neq 0$，则 $A_q\left(b_{i,j}\right)$ 是 $GF(q)$ 上的一个 α 倍循环置换矩阵；若 $b_{i,j}=0$，则 $A_b\left(b_{i,j}\right)$ 是一个全零矩阵。

H_b 和 H_q 分别是 $GF(2)$、$GF(q)$ 上的一个 $m(q-1)\times n(q-1)$ 矩阵，将其分别称矩阵 B 的 $(q-1)$ 重二进制和 q 进制阵列散列((q-1)-fold binary and q-ary array dispersions)。

对于任意整数对 γ 和 ρ，$1\leq\gamma\leq m$ 且 $1\leq\rho\leq n$，令 $H_b(\gamma,\rho)$ 和 $H_q(\gamma,\rho)$ 分别表示 H_b 和 H_q 的一个 $\gamma\times\rho$ 子阵列，则 $H_b(\gamma,\rho)$ 和 $H_q(\gamma,\rho)$ 分别是 $GF(2)$、$GF(q)$ 上的一个 $\gamma(q-1)\times\rho(q-1)$ 矩阵。$H_b(\gamma,\rho)$ 在 $GF(2)$ 上的零空间给出了一个二进制 QC-LDPC 码 C_b，类似地，$H_q(\gamma,\rho)$ 在 $GF(q)$ 上的零空间给出了一个 q 进制 QC-LDPC 码 C_q，其码长均为 $(q-1)\rho$。若 $H_b(\gamma,\rho)$ 和 $H_q(\gamma,\rho)$ 均不包含全零矩阵，则其具有固定的行重 γ 和列重 ρ，码 C_b 和 C_q 均是规则的，反之，它们均为非规则的。

定理 3：如果矩阵 B 满足 2×2 子矩阵约束，则 H_b、H_q 满足 RC-约束(Row-column constraint)，即 H_b、H_q 中任意两行(或两列)至多有一个对应位置都为非零项。

证明：假设 H_b 不满足 RC-约束。因为 H_b 是一个循环置换矩阵的阵列，所以存在 i,j,s,t,k,l，其中 $0\leq i,j<m$ 且 $i\neq j$，$0\leq s,t<n$ 且 $s\neq t$，$0\leq k,l<q-1$，使得 $A_b\left(b_{i,s}\right)$ 的第 k 行与 $A_b\left(b_{j,s}\right)$ 的第 l 行相等，即 $z_b\left(\alpha^k b_{i,s}\right)=z_b\left(\alpha^l b_{j,s}\right)$；且 $A_b\left(b_{i,t}\right)$ 的第 k 行与 $A_b\left(b_{j,t}\right)$ 的第 l 行相等，即 $z_b\left(\alpha^k b_{i,t}\right)=z_b\left(\alpha^l b_{j,t}\right)$。因为在

$GF(q)$上不同的元素有不同的位置向量，所以$\alpha^k b_{i,s}=\alpha^l b_{j,s}$且$\alpha^k b_{i,t}=\alpha^l b_{j,t}$。因此$\alpha^k b_{i,s}\alpha^l b_{j,t}=\alpha^k b_{i,t}\alpha^l b_{j,s}$，即$b_{i,s}b_{j,t}=b_{i,t}b_{j,s}$，与矩阵$B$满足$2\times 2$子矩阵约束矛盾，故$H_b$满足RC-约束。同理，可证$H_q$也满足RC-约束。

4. 基于有限域构造SC-QC-LDPC码的一般方法

考虑$GF(q)$上一个满足2×2子矩阵约束$m\times n$矩阵$B=\left[b_{i,j}\right]_{0\le i<m,0\le j<n}$，复制矩阵$B$形成$B$的一个二维半无限阵列$B_{rep}$：

$$B_{rep}=\left[b_{rep,i,j}\right]_{0\le i,j<\infty}=\begin{bmatrix}B & B & B & \cdots\\ B & B & B & \cdots\\ B & B & B & \cdots\\ \vdots & \vdots & \vdots & \ddots\end{bmatrix},$$

其中对于任意$i,j\ge 0$；$b_{rep,i,j}=b_{(i \bmod m),(j \bmod n)}$。其次，构造一个具有带对角线结构的$s\times t$修饰矩阵$W_{base}=\left[w_{base,i,j}\right]_{0\le i<s,0\le j<t}$，使用$W_{base}$修饰$B_{rep}(s,t)$形成一个SC基矩阵$B_{sc}=B_{rep}(s,t)\circ W_{base}$。最后，利用$B_{sc}$的二进制阵列散列形成一个$GF(2)$上的$s(q-1)\times t(q-1)$矩阵$H_{sc,qc,b}$，其零空间给出一个二进制SC-QC-LDPC码$C_{sc,qc,b}$；类似地，利用$B_{sc}$的$q$进制阵列散列形成一个$GF(q)$上的$s(q-1)\times t(q-1)$矩阵$H_{sc,qc,q}$，其零空间给出一个$q$进制SC-QC-LDPC码$C_{sc,qc,q}$。

算法1 基于有限域二进制SC-QC-LDPC码的构造

Step 1：构造$GF(q)$上一个满足2×2子矩阵约束$m\times n$矩阵$B=\left[b_{i,j}\right]_{0\le i<m,0\le j<n}$；

Step 2：复制矩阵B形成B的一个二维半无限阵列B_{rep}：

$$B_{rep}=\left[b_{rep,i,j}\right]_{0\le i,j<\infty}=\begin{bmatrix}B & B & B & \cdots\\ B & B & B & \cdots\\ B & B & B & \cdots\\ \vdots & \vdots & \vdots & \ddots\end{bmatrix},$$

其中对于任意$i,j\ge 0$；$b_{rep,i,j}=b_{(i \bmod m),(j \bmod n)}$；

Step 3：构造一个具有带对角线结构的$s\times t$修饰矩阵$W_{base}=\left[w_{base,i,j}\right]_{0\le i<s,0\le j<t}$；

Step 4：使用W_{base}修饰$B_{rep}(s,t)$形成一个SC基矩阵$B_{sc}=B_{rep}(s,t)$；

Step 5：利用B_{sc}的二进制阵列散列形成一个$GF(2)$上的$s(q-1)\times t(q-1)$矩阵$H_{sc,qc,b}$，其零空间给出一个二进制SC-QC-LDPC码$C_{sc,qc,b}$。

算法2 基于有限域多进制SC-QC-LDPC码的构造

Step 1：构造$GF(q)$上一个满足2×2子矩阵约束$m\times n$矩阵$B=\left[b_{i,j}\right]_{0\le i<m,0\le j<n}$；

Step 2：复制矩阵B形成B的一个二维半无限阵列B_{rep}：

$$B_{rep}=\left[b_{rep,i,j}\right]_{0\le i,j<\infty}=\begin{bmatrix}B & B & B & \cdots\\ B & B & B & \cdots\\ B & B & B & \cdots\\ \vdots & \vdots & \vdots & \ddots\end{bmatrix},$$

其中对于任意$i,j\ge 0$；$b_{rep,i,j}=b_{(i \bmod m),(j \bmod n)}$；

Step 3：构造一个具有带对角线结构的$s\times t$修饰矩阵$W_{base}=\left[w_{base,i,j}\right]_{0\le i<s,0\le j<t}$；

Step 4：使用W_{base}修饰$B_{rep}(s,t)$形成一个SC基矩阵$B_{sc}=B_{rep}(s,t)$；

Step 5：利用B_{sc}的q进制阵列散列形成一个$GF(q)$上的$s(q-1)\times t(q-1)$矩阵$H_{sc,qc,q}$，其零空间给出一个q进制SC-QC-LDPC码$C_{sc,qc,q}$。

在原模图构造中，我们可以把修饰矩阵 W_{base} 看作是与 SC 原模图相对应的原模矩阵(每对变量节点(Variable node, VN)和校验节点(Check node, CN)之间的边数不超过 1)。此外，上述结构等价于提升 W_{base} 相对应的 SC 原模图，其提升因子为 $q-1$。然而，提升(边的置换)是使用代数方法进行的。更一般地，这种构造也可以看作是 SC-LDPC 码的叠加构造[21]，叠加基矩阵与修饰矩阵 W_{base} 完全相同。

对于给定的修饰矩阵 W_{base}，我们可以得出最终的 SC-QC-LDPC 码的校验矩阵 $H_{sc,qc}$ 完全取决于 B 的选择。下面的定理是关于 B 的选择如何影响最终的 SC-QC-LDPC 码的围长性质。

定理 4：假设 B 是 $GF(q)$ 上一个满足 2×2 子矩阵约束的 $m\times n$ 矩阵，且 $B_{sc}=B_{rep}(s,t)\circ W_{base}$。对于任意的 i_1,i_2,j_1,j_2 使得 $w_{base,i_1,j_1}=w_{base,i_1,j_2}=w_{base,i_2,j_1}=w_{base,i_2,j_2}=1$，若 i_1-i_2、j_1-j_2 分别不能被 m、n 整除，则 B_{sc} 满足 2×2 子矩阵约束。

证明：假设 B_{sc} 不满足 2×2 子矩阵约束，则存在 i_1,i_2,j_1,j_2，使得 $B_{sc,i_1,j_1}B_{sc,i_2,j_2}=B_{sc,i_2,j_1}B_{sc,i_1,j_2}$，且 $w_{base,i_1,j_1}=w_{base,i_1,j_2}=w_{base,i_2,j_1}=w_{base,i_2,j_2}=1$。再根据 B 和 $B_{rep}(s,t)$ 的关系，可得出 i_1-i_2、j_1-j_2 分别能被 m、n 整除，矛盾。因此，B_{sc} 满足 2×2 子矩阵约束。

上述二进制和多进制 SC-QC-LDPC 码的结构是基于 $GF(q)$ 上基矩阵 B 的 $(q-1)$ 重二进制矩阵散列或 q 进制矩阵散列和修饰矩阵 W_{base} 构造，其中基矩阵 B 满足 2×2 子矩阵约束。现在的问题是如何构造基矩阵 B 和修饰矩阵 W_{base}。接下来的三节将研究上述问题。

5. 基于有限域本原元的 SC-QC-LDPC 码构造

基矩阵 B 的构造：

对于 $0<u<q-1$，当且仅当 u 和 $q-1$ 互素，$GF(q)$ 上的非零元素 α^u 是一个本原元。$GF(q)$ 中本原元的个数 K 可由下式给出的欧拉函数确定，其中 $p_1,p_2,\cdots,p_k$ 是 $q-1$ 的不同素因子。

$$K=(q-1)\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

设 $\{\alpha^{u_1},\alpha^{u_2},\cdots,\alpha^{u_K}\}$ 是 $GF(q)$ 中 K 个本原元组成的集合，令 $u_0=0$。构造 $GF(q)$ 上的 $(K+1)\times(K+1)$ 矩阵：

$$B^{(1)}=\begin{bmatrix}b_0\\b_1\\\vdots\\b_{m-1}\end{bmatrix}=\begin{bmatrix}\alpha^{u_0-u_0}-1 & \alpha^{u_1-u_0}-1 & \cdots & \alpha^{u_K-u_0}-1\\ \alpha^{u_0-u_1}-1 & \alpha^{u_1-u_1}-1 & \cdots & \alpha^{u_K-u_1}-1\\ \vdots & \vdots & \ddots & \vdots\\ \alpha^{u_0-u_K}-1 & \alpha^{u_1-u_K}-1 & \cdots & \alpha^{u_K-u_K}-1\end{bmatrix} \tag{5.1}$$

由上式，可以看出，矩阵 $B^{(1)}$ 具有以下结构性质：1) 每一行(列)的所有元素在 $GF(q)$ 上是不同的元素；2) 每一行(列)包含一个有且仅有一个零元素；3) 任何两行(列)对应位置上的元素均不同；4) $K+1$ 个 0 元素均位于矩阵的主对角线上。

推论 1：矩阵 $B^{(1)}$ 满足 2×2 子矩阵约束。

证明：基于定理 1 和定理 2，对于矩阵 $B^{(1)}$ 的任意 2×2 子矩阵 $B_{2\times 2}^{(1)}$，其元素属于第 i_1 行、第 i_2 行和第 j_1 列、第 j_2 列，其中 $0\le i_1,i_2,j_1,j_2\le K+1$ 且 $i_1\ne i_2$、$j_1\ne j_2$，其行列式

$$\det\left(B_{2\times 2}^{(1)}\right)=\left(\alpha^{u_{j_1}-u_{i_1}}-1\right)\left(\alpha^{u_{j_2}-u_{i_2}}-1\right)-\left(\alpha^{u_{j_2}-u_{i_1}}-1\right)\left(\alpha^{u_{j_1}-u_{i_2}}-1\right)=\frac{\left(\alpha^{u_{i_1}}-\alpha^{u_{i_2}}\right)\left(\alpha^{u_{j_1}}-\alpha^{u_{j_2}}\right)}{\alpha^{u_{i_1}+u_{i_2}}}\ne 0$$

，因此，矩阵 $B^{(1)}$ 满足 2×2 子矩阵约束。

因此，$B^{(1)}$ 可作为进行 $(q-1)$ 重阵列散列的基矩阵来构造二进制和多进制 SC-QC-LDPC 码。

修饰矩阵 W_{base} 的构造：

基于定理 4，选取一个具有 SC 结构原模图的原模矩阵[22]作为修饰矩阵来修饰基矩阵 B。

$$B=\begin{bmatrix}3 & 3\end{bmatrix}\Rightarrow B_0=B_1=B_2=\begin{bmatrix}1 & 1\end{bmatrix}$$

下面以几个例子来说明基于有限域本原元的 SC-QC-LDPC 码的构造。

5.1. 一类二进制 SC-QC-LDPC 码

例 5.1.

基矩阵 B 的选取：将 $GF\left(2^8\right)$ 作为构造码的域。注意到 $2^8-1=255$ 可分解为 $3\times5\times17$。根据欧拉方程可知 $GF\left(2^8\right)$ 有 $K=255\times\left(1-1/3\right)\left(1-1/5\right)\left(1-1/17\right)=128$ 个本原元。利用式(5.1)，我们可以构造一个 128 × 128 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=40$，$a=3$，$b=2$，$c=1$，且选择 40 个分量规则矩阵 $\left\{\Delta_k\right\}\left(0\le k\le4\right)$ 为全一矩阵。

二进制 SC-QC-LDPC 码的构造：利用算法 1 给出的构造方法，可形成一个 $GF\left(2\right)$ 上的 5334 × 10,160 矩阵 $H_{sc,qc,b}$，其零空间给出一个二进制 SC-QC-LDPC 码 $C_{sc,qc,b}$。

5.2. 一类多进制 SC-QC-LDPC 码

例 5.2.

基矩阵 B 的选取：将 $GF\left(2^6\right)$ 作为构造码的域。注意到 $2^6-1=63$ 可分解为 $3\times3\times7$。根据欧拉方程可知 $GF\left(2^8\right)$ 有 $K=63\times\left(1-1/3\right)\left(1-1/7\right)=36$ 个本原元。利用式(5.1)，我们可以构造一个 36 × 36 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=40$，$a=3$，$b=2$，$c=1$，且选择 40 个分量规则矩阵 $\left\{\Delta_k\right\}\left(0\le k\le4\right)$ 为全一矩阵。

多进制 SC-QC-LDPC 码的构造：利用算法 2 给出的构造方法，可形成一个 $GF\left(q\right)$ 上 2646 × 5040 矩阵 $H_{sc,qc,q}$，其零空间给出一个 q 进制 SC-QC-LDPC 码 $C_{sc,qc,q}$。

6. 基于有限域的加法子群构造 SC-QC-LDPC 码

基矩阵 B 的构造：令 $q=p^m$，其中 p 为素数且 m 为正整数。设 $GF\left(q\right)$ 是素域 $GF\left(q\right)$ 扩域，α 是 $GF\left(q\right)$ 的本原元，则 $\alpha^0,\alpha^1,\cdots,\alpha^{m-1}$ 在 $GF\left(q\right)$ 上线性无关，它们构成了 $GF\left(q\right)$ 的一组基。$GF\left(q\right)$ 的任意元素 α^i 都可以表示为 $\alpha^0,\alpha^1,\cdots,\alpha^{m-1}$ 的线性组合，即 $\alpha^i=c_{i,0}\alpha^0+c_{i,1}\alpha+\cdots+c_{i,m-1}\alpha^{m-1}$，其中，$c_{i,j}\in GF\left(p\right)$。当 $1\le t<m$ 时，设 $G_1=\left\{\beta_0=0,\beta_1,\cdots,\beta_{p^t-1}\right\}$ 是由 $\alpha^0,\alpha^1,\cdots,\alpha^t$ 的线性组合生成的 $GF\left(q\right)$ 上的加法子群，即 $\beta^i=c_{i,0}\alpha^0+c_{i,1}\alpha+\cdots+c_{i,t}\alpha^t$，其中，$c_{i,j}\in GF\left(p\right)$。设 $G_2=\left\{\gamma_0=0,\gamma_1,\cdots,\gamma_{p^{m-t}-1}\right\}$ 是由 $\alpha^t,\alpha^{t+1},\cdots,\alpha^{m-1}$ 的线性组合生成的 $GF\left(q\right)$ 上的加法子群，即 $\gamma^i=c_{i,t}\alpha^t+c_{i,t+1}\alpha^{t+1}+\cdots+c_{i,m-1}\alpha^{m-1}$，其中，$c_{i,j}\in GF\left(p\right)$。显然，$G_1\bigcap G_2=\left\{0\right\}$。当 $0\le i<p^{m-t}$ 时，定义如下元素集合：

$$\gamma_i+G_1=\left\{\gamma_i,\gamma_i+\beta_1,\cdots,\gamma_i+\beta_{p^t-1}\right\}$$

该集合其实就是以 γ_i 为陪集首的 G_1 的陪集，包括其自身。这 P^{m-t} 个陪集构成了有限域 $GF\left(q\right)$ 中 q 个元素的一个划分。G_1 的两个陪集是不相交的。

构造 $GF\left(q\right)$ 上大小为 $p^{m-t}\times p^t$ 的矩阵：

$$B^{(2)}=\begin{bmatrix}b_0\\b_1\\\vdots\\b_{m-1}\end{bmatrix}=\begin{bmatrix}0 & \beta_1 & \cdots & \beta_{p^t-1}\\\gamma_1 & \gamma_1+\beta_1 & \cdots & \gamma_1+\beta_{p^t-1}\\\vdots & \vdots & \ddots & \vdots\\\gamma_{p^{m-t}-1} & \gamma_{p^{m-t}}+\beta_1 & \cdots & \gamma_{p^{m-t}}+\beta_{p^t-1}\end{bmatrix}\tag{6.1}$$

这里对于$0 \le i < P^{m-t}$，第 i 行由 G_1 的第 i 个陪集的元素组成。$GF(q)$ 的每一个元素在 $B^{(2)}$ 中出现且仅出现一次。除第一行，$B^{(2)}$ 中的每一行 b_i 都由 $GF(q)$ 的非零元素组成。$B^{(2)}$ 的第一行第一个位置为 $GF(q)$ 上的 0 元素。除第一列，$B^{(2)}$ 中的每一行都由 $GF(q)$ 的非零元素组成。$B^{(2)}$ 的第一列第一个位置为 $GF(q)$ 上的 0 元素。由于 G_1 的任意两个陪集互不相交，故 $B^{(2)}$ 任意不同两行对应位置的元素也互不相同。

推论 2：矩阵 $B^{(2)}$ 满足 2×2 子矩阵约束。

证明：基于定理 1 和定理 2，对于矩阵 $B^{(2)}$ 的任意 2×2 子矩阵 $B_{2\times 2}^{(2)}$，其元素属于第 i_1 行、第 i_2 行和第 j_1 列、第 j_2 列，其中 $0 \le i_1, i_2 \le P^{m-t}$、$0 \le j_1, j_2 \le P^t$ 且 $i_1 \ne i_2$、$j_1 \ne j_2$，其行列式 $\det\left(B_{2\times 2}^{(2)}\right) = \left(\gamma_{i_1} + \beta_{j_1}\right)\left(\gamma_{i_2} + \beta_{j_2}\right) - \left(\gamma_{i_1} + \beta_{j_2}\right)\left(\gamma_{i_2} + \beta_{j_1}\right) = \left(\gamma_{i_1} - \gamma_{i_2}\right)\left(\beta_{j_1} - \beta_{j_2}\right) \ne 0$，因此，矩阵 $B^{(2)}$ 满足 2×2 子矩阵约束。

修饰矩阵 W_{base} 的构造：

基于定理4，选取一个码率为 1/3 的结构化不规则 LDPC 码的原模图，其相对应的原模矩阵为：

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

为了保持原结构化不规则分组码的度分布，使用展开技术(unwrapping technique)来构造修饰矩阵 W_{base}。将 V 分解为两个矩阵 V_1 和 V_2，使得 $V = V_1 + V_2$，其中

$$V_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix},$$

$$V_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix},$$

则

$$W_{base} = \begin{bmatrix} V_1 & & & & & \\ V_2 & V_1 & & & & \\ & V_2 & V_1 & & & \\ & & V_2 & & & \\ & & & \ddots & & \\ & & & \ddots & V_1 & \\ & & & & V_2 & \end{bmatrix} \tag{6.2}$$

下面以几个例子来说明基于有限域的加法子群 SC-QC-LDPC 码的构造。

6.1. 一类二进制 SC-QC-LDPC 码

例 6.1.

基矩阵 B 的选取：将 $GF\left(2^8\right)$ 作为构造码的域。令 α 为 $GF\left(2^8\right)$ 的本原元($GF\left(2\right)$ 的一个扩域)。设 $t=5$，则 $m-t=3$。设 G_1 和 G_2 是 $GF\left(2^8\right)$ 上加法群的两个子群，分别由 $\left\{\alpha^0,\alpha^1,\alpha^2,\alpha^3,\alpha^4\right\}$ 和 $\left\{\alpha^5,\alpha^6,\alpha^7\right\}$ 张成。因此 $G_1=\left\{\beta_0=0,\beta_1,\cdots,\beta_{31}\right\}$，$G_2=\left\{\gamma_0=0,\gamma_1,\cdots,\gamma_7\right\}$。利用式(6.1)，我们可以构造一个 8 × 32 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=26$，利用式(6.2)，我们可以构造一个 162 × 208 修饰矩阵 W_{base}。

二进制 SC-QC-LDPC 码的构造：利用算法 1 给出的构造方法，可形成一个 $GF\left(2\right)$ 上 20,574 × 26,416 矩阵 $H_{sc,qc,b}$，其零空间给出一个二进制 SC-QC-LDPC 码 $C_{sc,qc,b}$。

6.2. 一类多进制 SC-QC-LDPC 码

例 6.2.

基矩阵 B 的选取：将 $GF\left(2^6\right)$ 作为构造码的域。令 α 为 $GF\left(2^6\right)$ 的本原元($GF\left(2\right)$ 的一个扩域)。设 $t=4$，则 $m-t=2$。设 G_1 和 G_2 是 $GF\left(2^6\right)$ 上加法群的两个子群，分别由 $\left\{\alpha^0,\alpha^1,\alpha^2,\alpha^3\right\}$ 和 $\left\{\alpha^4,\alpha^5\right\}$ 张成。因此 $G_1=\left\{\beta_0=0,\beta_1,\cdots,\beta_{15}\right\}$，$G_2=\left\{\gamma_0=0,\gamma_1,\gamma_2,\gamma_3\right\}$。利用式(6.1)，我们可以构造一个 4 × 16 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=26$，利用式(6.2)，我们可以构造一个 162 × 208 修饰矩阵 W_{base}。

多进制 SC-QC-LDPC 码的构造：利用算法 2 给出的构造方法，可形成一个 $GF\left(q\right)$ 上 10,206 × 13,104 矩阵 $H_{sc,qc,q}$，其零空间给出一个 q 进制 SC-QC-LDPC 码 $C_{sc,qc,q}$。

7. 基于有限域的乘法子群构造 SC-QC-LDPC 码

基矩阵 B 的构造：令 α 是 $GF\left(q\right)$ 的本原元。假设 $q-1$ 不是素数。令 $\beta=\alpha^k$，$\gamma=\alpha^m$，其中 k、m 互素且 $q-1=km$，则 $M_1=\left\{\beta^0=1,\beta,\cdots,\beta^{m-1}\right\}$ 和 $M_2=\left\{\gamma^0=1,\gamma,\cdots,\gamma^{k-1}\right\}$ 构成了 $GF\left(q\right)$ 上的两个循环乘法子群，且 $M_1\bigcap M_2=\left\{1\right\}$。当 $0\le i<k$，集合 $\gamma^iM_1=\left\{\gamma^i,\gamma^i\beta,\cdots,\gamma^i\beta^{m-1}\right\}$ 是 M_1 的一个乘法陪集。循环子群 M_1 共有 k 个乘法陪集，包括其自身。当 $0\le j<m$，集合 $\beta^jM_2=\left\{\beta^j,\beta^j\gamma,\cdots,\beta^j\gamma^{k-1}\right\}$ 是 M_2 的一个乘法陪集。循环子群 M_2 共有 m 个乘法陪集，包括其自身。构造 $GF\left(q\right)$ 上大小为 $k\times m$ 的矩阵：

$$B^{(3)}=\begin{bmatrix}b_0\\b_1\\\vdots\\b_{m-1}\end{bmatrix}=\begin{bmatrix}0&\beta-1&\cdots&\beta^{m-1}-1\\\gamma-1&\gamma\beta-1&\cdots&\gamma\beta^{m-1}-1\\\vdots&\vdots&\ddots&\vdots\\\gamma^{k-1}-1&\gamma^{k-1}\beta-1&\cdots&\gamma^{k-1}\beta^{m-1}-1\end{bmatrix}\tag{7.1}$$

其中，第 i 行的分量可通过将 M_1 的第 i 个乘法陪集中每一个元素减去 $GF\left(q\right)$ 中的元素 1 得到的；第 j 行的分量可通过将 M_2 的第 j 个乘法陪集中每一个元素减去 $GF\left(q\right)$ 中的元素 1 得到的。

由上式，可以看出，矩阵 $B^{(1)}$ 具有以下结构性质：1) 有且仅有一个 0 元素，其位于左上角，其余 $km-1$ 个元素均是 $GF\left(q\right)$ 上的非零元素；2) 任意两行的 m 个对应位置上的元素均不相同；3) 任意两列的 k 个对应位置上的元素均不相同；4) 所有元素均是 $GF\left(q\right)$ 上的不同元素。

推论 3：矩阵 $B^{(3)}$ 满足 2×2 子矩阵约束。

证明：基于定理 1 和定理 2，对于矩阵 $B^{(3)}$ 的任意 2×2 子矩阵 $B_{2\times2}^{(3)}$，其元素属于第 i_1 行、第 i_2 行和第 j_1 列、第 j_2 列，其中 $0\le i_1,i_2\le k$、$0\le j_1,j_2\le m$ 且 $i_1\ne i_2$、$j_1\ne j_2$，其行列式 $\det\left(B_{2\times2}^{(3)}\right)=\left(\gamma^{i_1}\beta^{j_1}-1\right)\left(\gamma^{i_2}\beta^{j_2}-1\right)-\left(\gamma^{i_1}\beta^{j_2}-1\right)\left(\gamma^{i_2}\beta^{j_1}-1\right)=\left(\gamma^{i_1}-\gamma^{i_2}\right)\left(\beta^{j_2}-\beta^{j_1}\right)\ne0$，因此，矩阵 $B^{(3)}$ 满足 2×2 子矩阵约束。

修饰矩阵 W_{base} 的构造：

基于定理 4，选取一个结构化不规则 LDPC 码的原模图，其相对应的原模矩阵为：

$$V^{*}=\begin{bmatrix}1&2&1&1&0&0&0&0\\0&1&1&0&0&0&0&0\\0&1&1&0&1&0&0&0\\0&1&1&1&0&1&0&0\\0&1&0&1&1&0&1&1\\0&0&1&1&0&1&1&1\end{bmatrix},$$

将多边原模图分解成二进制矩阵之和，将 V 分解为 V_3 和 V_4，使得 $V^{*}=V_3+V_4$，其中

$$V_3=\begin{bmatrix}1&1&1&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&1&0&0&1&0&0&0\\0&1&0&1&0&0&0&0\\0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\end{bmatrix},$$

$$V_4=\begin{bmatrix}0&1&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&1&0&0&1&0&0\\0&0&0&1&0&0&0&1\\0&0&0&1&0&0&1&0\end{bmatrix},$$

利用使用展开技术(unwrapping technique)来构造修饰矩阵 W_{base}：

$$W_{base}=\begin{bmatrix}V_3&&&&&&\\V_4&V_3&&&&&\\&V_4&V_3&&&&\\&&V_4&&&&\\&&&\ddots&&&\\&&&&\ddots&V_3&\\&&&&&V_4\end{bmatrix}. \tag{7.2}$$

下面以几个例子来说明基于有限域的乘法子群 SC-QC-LDPC 码的构造。

7.1. 一类二进制 SC-QC-LDPC 码

例 7.1.

基矩阵 B 的选取：将 $GF\left(2^8\right)$ 作为构造码的域。令 α 为 $GF\left(2^8\right)$ 的本原元($GF\left(2\right)$ 的一个扩域)。可以看到，$2^8-1=255$，其可以分解为 5 和 51 的乘积，且它们互素。令 $\beta=\alpha^5$，$\gamma=\alpha^{51}$。集合 $M_1=\left\{\beta^0=1,\beta,\cdots,\beta^{50}\right\}$ 和 $M_2=\left\{\gamma^0=1,\gamma,\cdots,\gamma^4\right\}$ 构成了 $GF\left(q\right)$ 上的两个循环乘法子群，且 $M_1\cap M_2=\left\{1\right\}$。利用式(7.1)，我们可以构造一个 5 × 51 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=26$，利用式(7.2)，我们可以构造一个 162 × 208 修饰矩阵 W_{base}。

二进制 SC-QC-LDPC 码的构造：利用算法 1 给出的构造方法，可形成一个 $GF\left(2\right)$ 上 20,574 × 26,416 矩阵 $H_{sc,qc,b}$，其零空间给出一个二进制 SC-QC-LDPC 码 $C_{sc,qc,b}$。

7.2. 一类多进制 SC-QC-LDPC 码

例 7.2.

基矩阵 B 的选取：将 $GF\left(2^6\right)$ 作为构造码的域。令 α 为 $GF\left(2^6\right)$ 的本原元($GF\left(2\right)$ 的一个扩域)。可以看到， $2^6-1=63$，其可以分解为 7 和 9 的乘积，且它们互素。令 $\beta=\alpha^7$， $\gamma=\alpha^9$。集合 $M_1=\left\{\beta^0=1,\beta,\cdots,\beta^8\right\}$ 和 $M_2=\left\{\gamma^0=1,\gamma,\cdots,\gamma^6\right\}$ 构成了 $GF\left(q\right)$ 上的两个循环乘法子群，且 $M_1\bigcap M_2=\left\{1\right\}$。利用式(7.1)，我们可以构造一个 7×9 基矩阵 B。

修饰矩阵 W_{base} 的选取：选择 $L=26$，利用式(7.2)，我们可以构造一个 162×208 修饰矩阵 W_{base}。

多进制 SC-QC-LDPC 码的构造：利用算法 2 给出的构造方法，可形成一个 $GF\left(q\right)$ 上 $20{,}574\times 26{,}416$ 矩阵 $H_{sc,qc,q}$，其零空间给出一个 q 进制 SC-QC-LDPC 码 $C_{sc,qc,q}$。

8. 结论

本文提出了一种构造二进制和多进制 SC-QC-LDPC 码的一般方法，所提出的方法是基于在有限域 $GF\left(q\right)$ 上对满足 2×2 子矩阵约束的修饰基矩阵的阵列散列，由此导出的稀疏校验矩阵所对应的 Tanner 图的围长至少为 6。基于一般方法，本文提出了 3 种构造二进制和多进制 SC-QC-LDPC 码的特定方法，由此构造出了 6 类二进制 SC-QC-LDPC 码和多进制 SC-QC-LDPC 码。

参考文献

[1] Felstrom, A.J. and Zigangirov, K. (1999) Time-Varying Periodic Convolutional Codes with Low-Density Parity-Check Matrix. *IEEE Transactions on Information Theory*, **45**, 2181-2191. https://doi.org/10.1109/18.782171

[2] Gallager, R.G. (1962) Low-Density Parity-Check Codes. *IRE Transactions on Information Theory*, **8**, 21-28. https://doi.org/10.1109/TIT.1962.1057683

[3] Kudekar, S., Richardson, T. and Urbanke, R. (2011) Threshold Saturation via Spatial Coupling: Why Convolutional LDPC Ensembles Perform So Well over the BEC. *IEEE Transactions on Information Theory*, **57**, 803-834. https://doi.org/10.1109/TIT.2010.2095072

[4] Kudekar, S., Measson, C., Richardson, T. and Urbankez, R. (2010) Threshold Saturation on BMS Channels via Spatial Coupling. 6*th International Symposium on Turbo Codes and Iterative Information Processing*, Brest, 6-10 September 2010, 309-313. https://doi.org/10.1109/ISTC.2010.5613887

[5] Yedla, A., Jian, Y.-Y., Nguyen, P. and Pfifister, H. (2012) A Simple Proof of Threshold Saturation for Coupled Scalar Recursions. 2012 7*th International Symposium on Turbo Codes and Iterative Information Processing*, Gothenburg, 27-31 August 2012, 51-55. https://doi.org/10.1109/ISTC.2012.6325197

[6] Lentmaier, M., Sridharan, A., Costello Jr., D.J. and Zigangirov, K. (2010) Iterative Decoding Threshold for LDPC Convolutional Codes. *IEEE Transactions on Information Theory*, **56**, 5274-5289. https://doi.org/10.1109/TIT.2010.2059490

[7] Huang, K., Mitchell, D.G.M., Wei, L., Ma, X. and Costello, D. (2015) Performance Comparison of LDPC Block and Spatially Coupled Codes over GF(*q*). *IEEE Transactions on Communications*, **63**, 592-604. https://doi.org/10.1109/TCOMM.2015.2397433

[8] Iyengar, A., Papaleo, M., Siegel, P., Wolf, J., Vanelli-Coralli, A. and Corazza, G. (2012) Windowed Decoding of Protograph-Based LDPC Convolutional Codes over Erasure Channels. *IEEE Transactions on Information Theory*, **58**, 2303-2320. https://doi.org/10.1109/TIT.2011.2177439

[9] Andriyanova, I. and Graelli Amat, A. (2013) Threshold Saturation for Nonbinary SC-LDPC Codes on the Binary Erasure Channel. *IEEE Transactions on Information Theory*, **62**, 2622-2638. https://doi.org/10.1109/TIT.2016.2540800

[10] Pusane, A., Smarandache, R., Vontobel, P. and Costello, D. (2011) Deriving Good LDPC Convolutional Codes from LDPC Block Codes. *IEEE Transactions on Information Theory*, **57**, 835-857. https://doi.org/10.1109/TIT.2010.2095211

[11] Fossorier, M. (2004) Quasi Cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices. *IEEE Transactions on Information Theory*, **50**, 1788-1793. https://doi.org/10.1109/TIT.2004.831841

[12] Li, Z., Chen, L., Zeng, L., Lin, S. and Fong, W. (2005) Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check

Codes. *IEEE Transactions on Communications*, **53**, 1973-1973. https://doi.org/10.1109/TCOMM.2005.858628

[13] Chen, Y. and Parhi, K. (2004) Overlapped Message Passing for Quasi-Cyclic Low-Density Parity Check Codes. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, **51**, 1106-1113. https://doi.org/10.1109/TCSI.2004.826194

[14] Uchikawa, H. Kasai, K. and Sakaniwa, K. (2011) Design and Performance of Rate-Compatible Non-Binary LDPC Convolutional Codes. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E94**, 2135-2143.

[15] Ryan, W. and Lin, S. (2009) Channel Codes: Classical and Modern. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511803253

[16] Lan, L., Zeng, L., Tai, Y., Chen, L., Lin, S. and Abdel-Ghaffar, K. (2007) Construction of Quasi-Cyclic LDPC Codes for AWGN and Binary Erasure Channels: A Finite Field Approach. *IEEE Transactions on Information Theory*, **53**, 2429-2458. https://doi.org/10.1109/TIT.2007.899516

[17] Zhang, L., Huang, Q., Lin, S., Abdel-Ghaffar, K. and Blake, I.F. (2010) Quasi-Cyclic LDPC Codes: An Algebraic Construction, Rank Analysis, and Codes on Latin Squares. *IEEE Transactions on Communications*, **58**, 3126-3139. https://doi.org/10.1109/TCOMM.2010.091710.090721

[18] Dolecek, L., Divsalar, D., Sun, Y. and Amiri, B. (2014) Non-Binary Protograph-Based LDPC Codes: Enumerators, Analysis, and Designs, Information Theory. *IEEE Transactions on Information Theory*, **60**, 3913-3941. https://doi.org/10.1109/TIT.2014.2316215

[19] Chandrasetty, V.A., Johnson, S.J. and Lechner, G. (2013) Memory Efficient Decoders Using Spatially Coupled Quasi-Cyclic LDPC Codes. *Clinical Orthopaedics and Related Research*, arXiv:1305.5625

[20] Hu, X.-Y., Eleftheriou, E. and Arnold, D.-M. (2005) Regular and Irregular Progressive Edge-Growth Tanner Graphs. *IEEE Transactions on Information Theory*, **51**, 386-398. https://doi.org/10.1109/TIT.2004.839541

[21] Li, J., Liu, K., Lin, S., Abdel-Ghaffar, K. and Ryan, W.E. (2015) An Unnoticed Strong Connection between Algebraic-Based and Protograph-Based LDPC Codes. 2015 *Information Theory and Applications Workshop*, San Diego, 1-6 February 2015, 36-45. https://doi.org/10.1109/ITA.2015.7308964

[22] Wei, L., Koike-Akino, T., Mitchell, D., Fuja, T. and Costello, D.J. (2014) Threshold Analysis of Non-Binary Spatially-Coupled LDPC Codes with Windowed Decoding, in Information Theory (ISIT). 2014 *IEEE International Symposium on*, Honolulu, 29 June-4 July 2014, 881-885. https://doi.org/10.1109/ISIT.2014.6874959