2 多指针弹性缓冲器结构设计

四个读写指针同时寻址维持常半满状态的多指针弹性缓冲器按时钟域的不同可分为恢复时钟域和本地时钟域，SKP 的删除发生在恢复时钟域，而 SKP 的添加则发生在本地时钟域.如图 7 所示，多指针弹性缓冲器的结构设计可以分为 SKP 检测单元，串并转换单元，输入控制单元，写指针控制单元，存储器单元，同步单元，阈值检测单元，读指针控制单元，输出控制单元，并串转换单元，下面分别介绍各单元模块的功能作用.

2.1 SKP 检测单元

SKP 检测单元是检测输入控制单元和输出控制单元中 40 bit 数据每 10 bit 是否为 SKP 字符，可用 SKP1[3:0]、SKP2[3:0]表示，为 SKP 的添加、删除提供了标志，可通过组合逻辑电路来实现.

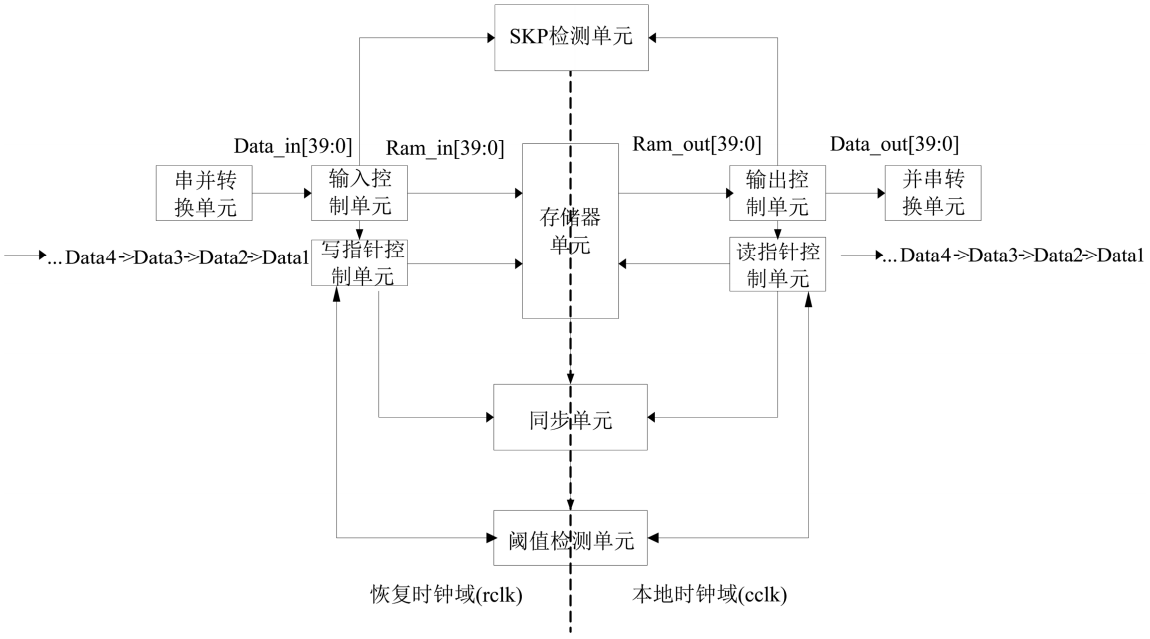

图 7 常半满模式弹性缓冲器结构

Fig.7 Elastic buffer structure with constant half full mode

2.2 串并转换单元

串并转换单元的功能是将连续输入的 4 个 10 bit 数据转换为单个 40 bit 的数据.

2.3 输入控制单元

输入控制单元的功能是改变输入的 40 bit 数据中相邻 10 bit 数据之间 SKP 字符与正常数据的排序.

2.4 写指针控制单元

写指针控制单元的功能是产生写指针及其格雷码，其中写指针用以选定写入的存储单元，并与同步后的读指针比较产生删除 SKP 请求标志.格雷码用于同步到读时钟域产生空标志及 SKP 添加请求标志.写使能信号有效时，写指针控制单元开始工作.若读写时钟频率一致，FIFO 中的有效数据将维持在 32 个.写指针的地址为 $w_3>=6'b111100$ 或者 $w_3<=6'b000010$ 时，则写指针根据 4 个指针当前地址位确定其在下个写时钟周期上升沿到来时的置位.

2.5 存储器单元

存储器单元是整个弹性缓冲器的基础，由于多指针弹性缓冲器用 4 个读写指针寻址，故设计的 FIFO 深度为 64，位宽为 10 bit.使用全局复位信号初始化存储单元，无需读写使能，选中即可读写数据.

2.6 同步单元

同步单元的作用是将写指针的格雷码同步到读时钟域，并与读指针格雷码比较，以产生空标志，这里的同步过程采用读时钟采样一次的方式实现.用同样的方法可将读指针同步到写时钟域，并与写指针格雷码比较，产生满标志.同时，同步单元还将同步后的读、写指针格雷码转换成二进制自然码输出.

2.7 阈值检测单元

阈值检测单元的作用是检测 FIFO 中有效数据的数量，并根据其数量与 32 的差值决定是否产生 SKP 添加/删除请求标志.为了避免亚稳态的产生，使用写时钟同步后的读指针与写指针比较产生 SKP 删除请求标志，经读时钟同步的写指针与读指针比较产生 SKP 添加请求标志，因为写指针总是先于读指针，所以差值由写指针(同步后)减去读指针

(同步后)产生.

2.8　读指针控制单元

读指针控制单元的主要功能是产生读指针及其格雷码,其中读指针用以选定要读出的存储单元,并于同步后的写指针比较产生添加 SKP 请求标志.格雷码用于同步到写时钟域产生满标志及 SKP 删除请求标志.读使能信号有效时,读指针控制单元开始工作.若读写时钟同步,FIFO 中的有效数据将维持在 32 个.若读指针的地址为 $r_3>=6'b111100$ 或者 $r_3<=6'b000010$,在下个读时钟周期上升沿到来时,读指针将依据 4 个指针当前不同的地址置位来确定.

2.9　输出控制单元

输出控制单元的功能为当缓冲器进行添加操作时,根据输出数据 SKP 对位置的不同改变输出的数据,添加 SKP 让输出数据不发生混乱.

2.10　串转换单元

并串转换单元的功能是将输出控制单元输出的 40 bit 的数据转换为 4 个 10 bit 的数据输出.

3　多指针弹性缓冲流程设计

多指针弹性缓冲器深度为 64,位宽为 10 bit,操作流程如图 8 和图 9 所示.图 8 是写指针操作流程.首先,写使能信号有效且复位信号为高电平,写指针开始工作,输入数据写入 FIFO,每个写指针地址加 4,完成数据的写操作;然后检测数据是否写满,如果数据写满,则写指针暂停一个时钟.如果数据不满,但写指针已经处于 $w_4>=6'b111100$ 或者 $w_4<=6'b000010$ 状态,则根据当前写指针位置,在下个时钟上升沿到来时对写指针进行置位.否则检测删除(Del)信号和输入数据的 SKP 标志是否有效,在其有效时,先通过输入控制单元调整输入的数据中 SKP 对的顺序,然后每个写指针地址加 2,完成删除操作.

图 9 是读指针操作流程.在读使能信号有效且复位信号置高时读指针开始工作,FIFO 中的数据通过读指针寻址读出,每个读指针地址加 4,完成数据读操作;然后检测读指针是否读空,读指针读空,则读指针暂停一个时钟;如果读指针非空且读指针已经处于 $r_4>=6'b111100$ 或者 $r_4<=6'b000010$ 的状态,则根据当前读指针位置;在下个时钟上升沿到来时对读指针进行置位.否则,检测添加信号和输出数据的 SKP 标志是否有效,若有效,先通过输出控制单元对输出的数据控制输出,然后每个读指针地址加 2,完成添加操作.

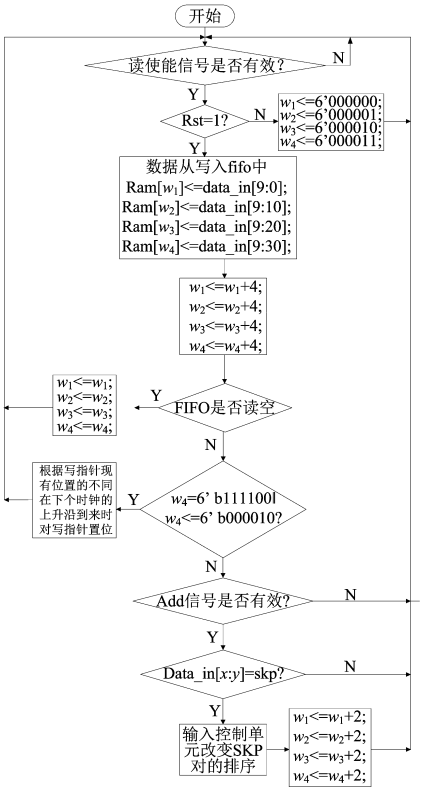

图 8　写操作流程设计图

Fig.8　Write pointer operation process

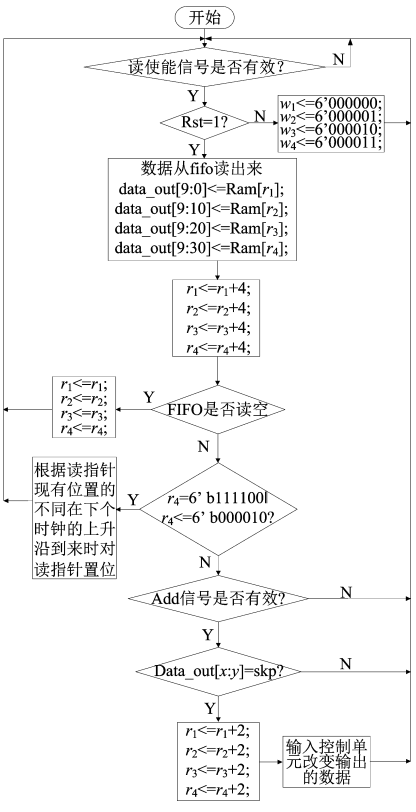

图 9　读操作流程设计图

Fig.9　Read pointer operation process

4 多指针弹性缓冲器的验证与测试

多指针弹性缓冲器在 Quartus Ⅱ 中完成 Verilog HDL 编程设计的输入、综合及时序约束，用 ModelSim 做功能仿真和时序仿真，时序仿真时选用的是 Altera 的 Cyclone-IV FPGA 的 EP4CE6F17C8N 芯片，给定 USB 3.0 协议要求下的频率，给定逻辑门延迟及高温的极端环境下仿真验证.得到的的波形如图 10～13 所示.图 10 表示 FIFO 中输入的数据含有 SKP 字符(of9，306)，且添加信号有效.图 11 表示读指针已经完成添加操作，输出数据中可以看到添加的 SKP 字符，并且添加信号已经由高跳变为低.图 12 表示输入的数据中含有 SKP 字符，写指针在删除信号有效时地址加 2 完成删除操作，删除信号在删除操作完成后由高跳变为低.图 13 表示输出的数据中 SKP 字符已经删除，维持了弹性缓冲器的常半满状态.通过测试可以看出，弹性缓冲器在读写指针频率不一致时，可以正确地完成 SKP 字符的添加和删除过程，维持缓冲器半满状态达到所设计的要求.

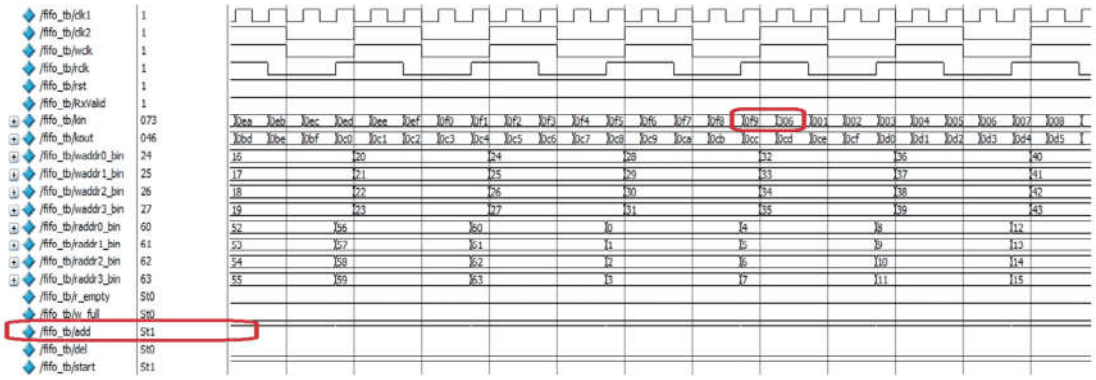

图 10 FIFO 中 SKP 添加信号有效且输入数据中有 SKP 字符

Fig.10 SKP adds the signal effectively and the input data has SKP characters In FIFO

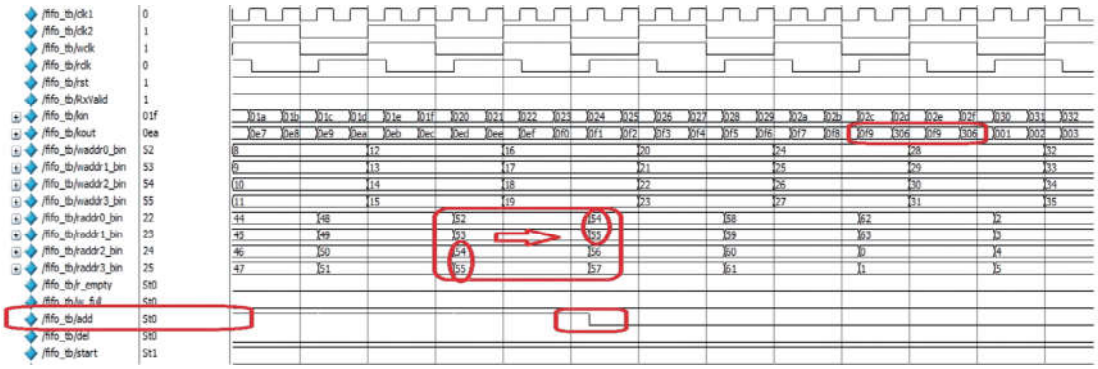

图 11 FIFO 中读指针变化、SKP 字符添加成功且添加使能信号变为低电平

Fig.11 Change of reading pointer in FIFO and the SKP character is added successfully and the enable signal is changed to low level

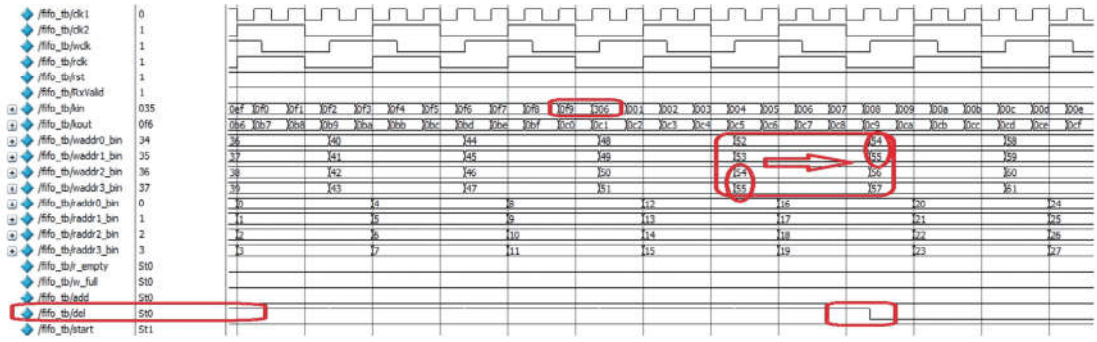

图 12 FIFO 中 SKP 删除信号有效且输入数据中有 SKP 字符

Fig.12 SKP delete signal valid in FIFO and the input data has SKP characters

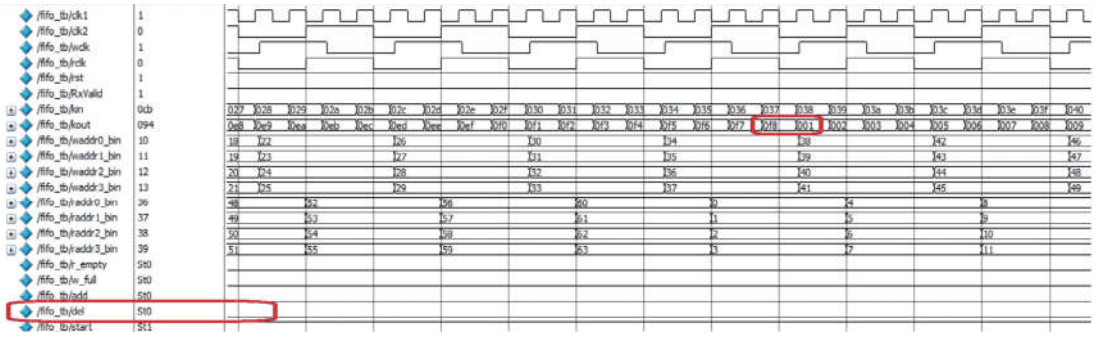

图 13　FIFO 中删除 SKP 字符

Fig.13　Deleting SKP characters in FIFO

5　结论

本文讨论了多指针弹性缓冲器的原理与实现方法，验证该弹性缓冲器可正确完成 SKP 特定字符的添加和删除，在 USB 3.0 协议规定的频率下能维持缓冲器在半满状态.本设计工作意义在于充分考虑了 USB3.0 协议对弹性缓冲器的高速率要求，在总时钟频率不变的情况下，采用 4 个读写指针同时读写数据，降低了 FIFO 中读写操作的频率，实现了弹性缓冲频率补偿的目的.另外，对本文设计的多指针弹性缓冲结构稍作修改就能应用于其他高速接口，因此本文的研究结论具有一定的工程应用价值.

参考文献(References)

[1] WINKLES J. Elastic buffer implementations in PCI express devices [EB/OL]. [2017-10-18], http://www. doc88. com/p-781379861436. html, Mindshare Inc.

[2] 彭琰，曾云，王太宏，等. 基于 HID 类 USB 外设功能控制器的 ASIC 设计[J]. 微电子学与计算机，2009，26(4)：15-18.

[3] Wikipedia. USB[EB/OL].[2011-09-28], http://en.wikipedia.org.

[4] 朱小明，王小力，程曾. USB3.0 物理层中弹性缓冲器的设计与实现[J]. 微电子学与计算机，2012，29(6)：117-121.

[5] 邢辉. 弹性缓冲在 USB3.0 物理层中设计与实现[EB/OL]. 北京：中国科技论文在线，2012.

[6] 廖艳，王广君，高杨. FPGA 异步时钟设计中的同步策略[J].自动化技术与应用，2006，25(1)：67-68.

[7] Universal Serial Bus 3.0 Specification. 112009004327.5 [P]. USA:HP Company，2008.

[8] 郑乾，晏敏，赵建中，等. 基于 PCIE2.0 的物理层弹性缓冲器设计[J]. 计算机工程，2014，40(10)：71-75.

[9] MICHELOGIANNAKIS G，BALFOUR J，DALLY W J. Elastic buffer flow control for On-chip Network [C]// The 15th International Symposium on High Performance Computer Architecture. Raleigh，USA：IEEE，2009：151-162.

[10] 刘奇浩，翁慧辉，张峰，等.65nm 工艺下基于 PCI Express2.0 协议的物理层编码子层设计[J].中国集成电路，2013，22(3)：41-45.

[11] WOODRAL D E. Elastic buffer module for PCI express devoices，7281077B2 [P]. USA，2007.

[12] CUMMINGS C E. Simulation and synthesis techniques for as synchronous FIFO design with asynchronous pointer comparisons [EB/OL]. [2017-10-18], http://read. pudn. com/downloads116/doc/495591/asyn _FIFO.pdf.

[13] 郑争兵. 基于 FPGA 的高速采样缓存系统的设计与实现[J]. 计算机应用，2012，32(11)：3259-3261.

文章编号:0253-2778(2017)10-0862-07

Skew cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1,\ v^3-v,\ uv-vu\rangle$

GUAN Yue, LIU Yan, SHI Minjia, LU Zhenyu, WU Bo

(*School of Mathematical Sciences, Anhui University. Hefei* 230601, *China*)

Abstract: The skew cyclic codes over $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q$ were conducted. By defining a gray map from R to $\mathbb{F}_q^6$, the gray image of a linear code of length n over R was considered. Moreover, the generator polynomials of skew cyclic codes over this ring were described and their structural properties by a decomposition theorem investigated. Further, it is shown that the skew cyclic codes over R are principally generated. Finally, the idempotent generators of skew cyclic codes over R were obtained.

Key words: linear codes; dual codes; skew cyclic codes; gray map

CLC number: TN911.22 **Document code**: A doi:10.3969/j.issn.0253-2778.2017.10.009

2010 Mathematics Subject Classification: Primary 94B05; Secondary 94B99

Citation: GUAN Yue, LIU Yan, SHI Minjia, et al. Skew cyclic codes over $\mathbb{F}_q[u,v]/\langle u^2-1,\ v^3-v,\ uv-vu\rangle$ [J]. Journal of University of Science and Technology of China, 2017,47(10):862-868.
管玥,刘艳,施敏加,等. 环 $\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码[J]. 中国科学技术大学学报,2017,47(10):862-868.

环 $\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码

管 玥,刘 艳,施敏加,卢振宇,吴 波

(安徽大学数学科学学院,安徽合肥 230601)

摘要: 研究了环 $R=\mathbb{F}_q[u,v]/\langle u^2-1,v^3-v,uv-vu\rangle$ 上的斜循环码.通过定义从 R 到 $\mathbb{F}_q^6$ 的 Gray 映射,考虑 R 上长度为 n 的线性码的 Gray 像.进一步,利用中国剩余定理定义了该环上的斜循环码并给出了它的生成多项式及结构特性.结果表明,R 上的斜循环码是主理想生成的.最后,给出了 R 上斜循环码的幂等生成元.

关键词: 线性码; 对偶码; 斜循环码; Gray 映射

Received: 2016-06-09; **Revised**: 2017-01-07

Foundation item: Supported by NNSF of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008), Natural Science Research Project of Higher Education of Anhui Province of China (KJ2015JD18).

Biography: GUAN Yue, female, born in 1994, Master candidate. Research field: algebra code. E-mail: guanyueeee@163.com

Corresponding author: SHI Minjia, PhD/Professor. E-mail: smjwcl.good@163.com

0 Introduction

A recent study presented by Boucher et al. introduced a noncommutative ring $\mathbb{F}_q[x,\theta]$, called skew polynomial ring, where $\mathbb{F}_q$ is a finite field with q elements and θ is a field automorphism of $\mathbb{F}_q$. Boucher et al.[1-2] considered the structure of cyclic codes closed under a skew cyclic shift over $\mathbb{F}_q[x,\theta]$, namely, skew cyclic codes, where the generator polynomials of skew cyclic codes come from the ring $\mathbb{F}_q[x,\theta]$. Further, they gave some examples of skew cyclic codes, the Hamming distances of which are larger than the best known linear codes with the same parameters. Based on that, a lot of researchers focused on skew cyclic codes. Recently, Cao[3] investigated the relation between quasi cyclic codes and skew polynomial rings. Boucher and Ulmer[4] introduced the factorization of skew polynomial in skew polynomial rings. These results allowed them to study the skew self-dual cyclic codes with length 2^s.

Later on, Abualrub et al.[5] defined skew quasi cyclic codes over these classes of rings . Jitman et al.[6] defined skew constacyclic codes by defining the skew polynomial ring with coefficients from finite chain rings, especially the ring $\mathbb{F}_{p^m}+u\mathbb{F}_{p^m}$ where $u^2=0$. Abualrub et al.[7] considered skew cyclic codes over the non chain ring $\mathbb{F}_2+v\mathbb{F}_2$ with $v^2=v$ by defining the automorphism $\theta_v: v\mapsto v+1$. However, Gao[8] generalized this result over $\mathbb{F}_p+v\mathbb{F}_p$. Gursoy et al.[9] investigated the structural properties of skew cyclic codes through the decomposition method over $\mathbb{F}_q+v\mathbb{F}_q$, where $v^2=v$ and $q=p^m$. In Ref.[10], the authors studied the structural properties of skew cyclic codes over the ring $\mathbb{F}_3+v\mathbb{F}_3$ with $v^2=1$ by considering the automorphism $\theta_v: v\mapsto -v$. They proved that skew cyclic codes over $\mathbb{F}_3+v\mathbb{F}_3$ are equivalent to either cyclic codes or quasi cyclic codes. A lot of work has been done in this direction such as Refs[11-12].

In this paper, we study skew cyclic codes defined by the skew polynomial ring with coefficients over the ring $R=\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q$. In our work, we consider the automorphisms $R\to R$, $a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2\mapsto a_1^{p^i}+a_2^{p^i}u+a_3^{p^i}v+a_4^{p^i}uv+a_5^{p^i}v^2+a_6^{p^i}uv^2$. The skew polynomial ring in our case is denoted by $R[x,\theta_i]$, where the addition is the usual polynomial addition and the multiplication is defined by the rule $xa=\theta_i(a)x$, $(a\in R)$.

1 Preliminary

Throughout this paper let R be the commutative ring $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q+v^2\mathbb{F}_q+uv^2\mathbb{F}_q=\{a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2$, where $a_j\in\mathbb{F}_q, 1\leqslant j\leqslant 6\}$ with $u^2=1, v^3=v$ and $uv=vu$. And R_1 denotes the non-chain ring $\mathbb{F}_q+u\mathbb{F}_q$ with $u^2=1$. Then $R=R_1+vR_1+v^2R_1$ can also be thought of as the quotient ring $\mathbb{F}_q[u,v]/\langle u^2-1, v^3-v, uv-vu\rangle$. It is easily checked that R is a Frobenius ring but not local. The definition of the Gray map from R to R_1^3 is defined as $\varphi(a+bv+cv^2)=(a, a+b+c, a-b+c)$, where $a, b, c\in R_1$. The Gray map φ_1 from R_1 to $\mathbb{F}_q^2$ is given by $\varphi_1(a+bu)=(a,b)$, where $a,b\in\mathbb{F}_q$. So we have the following definition.

Definition 1.1 The definition of the Gray map from R to $\mathbb{F}_q^6$ is given by $\Phi(a_1+a_2u+a_3v+a_4uv+a_5v^2+a_6uv^2)=(a_1, a_2, a_1+a_3+a_5, a_2+a_4+a_6, a_1-a_3+a_5, a_2-a_4+a_6)$, where $a_j\in\mathbb{F}_q$, $j=1,2,3,4,5,6$.

This map Φ can be extended to R^n in an obvious way. The Hamming distance $d_H(x,y)$ between two vectors x and y over $\mathbb{F}_q$ is the Hamming weight of the vector $x-y$, that is, $d_H(x,y)=w_H(x-y)$. The Lee weight $w_L(x)$ of $x=(x_0,x_1,\cdots,x_{n-1})\in R^n$ is defined as $w_L(x)=w_H(\Phi(x))$. For any $x,y\in R^n$, the Lee distance between x and y is given by $d_L(x,y)=w_L(x-y)$. A linear code C of length n over R is an R-submodule of R^n. It is easy to verify that the Gray image of a linear code over R is a q-ary linear code.

According to the definition of Lee distance, we have the following lemma.

Lemma 1.1 The Gray map Φ is a distance-preserving map from (R^n, Lee distance) to ($\mathbb{F}_q^{6n}$, Hamming distance) and this map is also $\mathbb{F}_q$-linear.

Proof It is clear that $\Phi(x-y)=\Phi(x)-\Phi(y)$ for $x,y\in R^n$. Thus, $d_L(x,y)=w_L(x-y)=w_H(\Phi(x-y))=w_H(\Phi(x)-\Phi(y))=d_H(\Phi(x),\Phi(y))$. Let $x,y\in R^n$, $k_1,k_2\in\mathbb{F}_q$, then from the definition of Gray map, we have $\Phi(k_1x+k_2y)=k_1\Phi(x)+k_2\Phi(y)$. This means that Φ is $\mathbb{F}_q$-linear.

Similar to Lemma 3.2 in Ref.[11] and combining Lemma 1.1, we have the following lemma.

Lemma 1.2 Let C be a linear code of length n over R with rank k and minimum Lee distance d, then $\Phi(C)$ is a $[6n, k, d]$ linear code over $\mathbb{F}_q$.

Proof From Lemma 1.1, we see that $\Phi(C)$ is an $\mathbb{F}_q$-linear code. What is more, we can easily obtain that $\Phi(C)$ has dimension k and length $6n$ since Φ is a bijective map from R^n to $\mathbb{F}_q^{6n}$. Note that the Gray map Φ is a distance-preserving map. So $\Phi(C)$ has the same minimum distance d. Let C be a linear code over R. The dual $C^\perp$ of C consists of all vectors of R^n which are orthogonal to every codeword in C. A code C is said to be self-dual (resp. self-orthogonal) if $C=C^\perp$ (resp. $C\subseteq C^\perp$). Let $x=(x_0,x_1,\cdots,x_{n-1})$ and $y=(y_0,y_1,\cdots,y_{n-1})$ be any two vectors over R^n, we define the usual Euclidean inner product by $x\cdot y=\sum_{i=0}^{n-1}x_iy_i$. An important connection that we want to investigate is the relation between the dual and the Gray image of a code. The following theorem resolves this issue.

Theorem 1.1 Let C be a linear code of length n over R. If $C^\perp$ is its dual, then $\Phi(C^\perp)=\Phi(C)^\perp$. Moreover, if C is self-dual, so is $\Phi(C)$ over $\mathbb{F}_q$.

Proof Let $c=(c_0,c_1,\cdots,c_{n-1})\in C$, where $c_i=c_{i1}+c_{i2}u+c_{i3}v+c_{i4}uv+c_{i5}v^2+c_{i6}uv^2$. Take $c'=(c'_0,c'_1,\cdots,c'_{n-1})\in C^\perp$, where $c'_i=c'_{i1}+c'_{i2}u+c'_{i3}v+c'_{i4}uv+c'_{i5}v^2+c'_{i6}uv^2$. Then we have $c=A_1+A_2u+A_3v+A_4uv+A_5v^2+A_6uv^2$ and $c'=B_1+B_2u+B_3v+B_4uv+B_5v^2+B_6uv^2$, where $A_j=(c_{0j},c_{1j},\cdots,c_{n-1\,j})$ and $B_j=(c'_{0j},c'_{1j},\cdots,c'_{n-1\,j})$ for $j=1,2,\cdots,6$. Since $c\cdot c'=0$ in R, then we have

$$\begin{aligned}
&A_1B_1+A_2B_2=0,\ A_1B_2+A_2B_1=0,\\
&A_1B_3+A_2B_4+A_3B_1+A_3B_5+A_4B_2+\\
&\qquad A_4B_6+A_5B_3+A_6B_4=0,\\
&A_1B_4+A_2B_3+A_3B_2+A_3B_6+A_4B_1+\\
&\qquad A_4B_5+A_5B_4+A_6B_3=0,\\
&A_1B_5+A_2B_6+A_3B_3+A_4B_4+A_5B_1+\\
&\qquad A_5B_5+A_6B_2+A_6B_6=0,\\
&A_1B_6+A_2B_5+A_3B_4+A_4B_3+A_5B_2+\\
&\qquad A_5B_6+A_6B_1+A_6B_5=0.
\end{aligned}$$

Note that $\Phi(c)\cdot\Phi(c')=0$, which implies $\Phi(C^\perp)\subseteq\Phi(C)^\perp$. Since $|C\,\|\,C^\perp|=|\Phi(C)|\,|\Phi(C)^\perp|=q^{6n}$ and $|\Phi(C^\perp)|=|C^\perp|$, then we get $|\Phi(C^\perp)|=|\Phi(C)^\perp|$. Hence $\Phi(C^\perp)=\Phi(C)^\perp$. If C is self-dual, then $\Phi(C)=\Phi(C^\perp)=\Phi(C)^\perp$.

2 Linear codes over R

By the Chinese Remainder Theorem, we have

$$\begin{aligned}
R=&(1-v^2)R\oplus(2^{-1}v+2^{-1}v^2)R\oplus\\
&(-2^{-1}v+2^{-1}v^2)R=\\
&(1-v^2)R_1\oplus(2^{-1}v+2^{-1}v^2)R_1\oplus\\
&(-2^{-1}v+2^{-1}v^2)R_1,
\end{aligned}$$

and $R_1=2^{-1}(1+u)\mathbb{F}_q\oplus2^{-1}(1-u)\mathbb{F}_q$. Hence $R=2^{-1}(1+u)(1-v^2)\mathbb{F}_q\oplus2^{-1}(1-u)(1-v^2)\mathbb{F}_q\oplus4^{-1}(1+u)(v+v^2)\mathbb{F}_q\oplus4^{-1}(1-u)(v+v^2)\mathbb{F}_q\oplus4^{-1}(1+u)(-v+v^2)\mathbb{F}_q\oplus4^{-1}(1-u)(-v+v^2)\mathbb{F}_q$. For the sake of convenience, we denote the elements in R by η_1, η_2, η_3, η_4, η_5, η_6 respectively, i.e., $\eta_1=2^{-1}(1+u)(1-v^2)$, $\eta_2=2^{-1}(1-u)(1-v^2)$, $\eta_3=4^{-1}(1+u)(v+v^2)$, $\eta_4=4^{-1}(1-u)(v+v^2)$, $\eta_5=4^{-1}(1+u)(-v+v^2)$, $\eta_6=4^{-1}(1-u)(-v+v^2)$. Note that η_j ($j=1,2,3,4,5,6$) are mutually orthogonal idempotents over R and $\sum_{j=1}^{6}\eta_j=1$. Let C be a linear code of length n over R. For $1\leqslant i\leqslant6$, define

$$\begin{aligned}
C_i=\{&\dot{x}_i\in\mathbb{F}_q^n\mid\exists\,\dot{x}_j\in\mathbb{F}_q^n,\ j=\{1,2,\cdots,6\}\backslash\{i\},\\
&\text{s.t.}\ \sum_{i=1}^{6}\eta_i\dot{x}_i\in C\}.
\end{aligned}$$

Then C_i ($i=1,2,\cdots,6$) are all linear codes of

length n over $\mathbb{F}_q$. Moreover, the code C of length n over R can be uniquely expressed as

$$C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6 \tag{1}$$

Let C, expressed as Eq.(1), be a linear code of length n with generator matrix G over R. Then, since C is an $\mathbb{F}_q$-module, the generator matrix G can be written as

$$G=\begin{pmatrix}\eta_1G_1\\ \eta_2G_2\\ \vdots\\ \eta_6G_6\end{pmatrix},$$

where G_1, G_2, G_3, G_4, G_5 and G_6 are the generator matrices of C_1, C_2, C_3, C_4, C_5 and C_6, respectively. Now, as an $\mathbb{F}_q$-module, the gray image of C under the Gray map Φ which is a module isomorphism, is an $\mathbb{F}_q$-subspace generated by $\Phi(G)$. So we can easily obtain the following corollary.

Corollary 2.1　Let C, expressed as (1), be a linear code of length n over R, then $d_H(\Phi(C))=\min\{d_H(C_1), d_H(C_2),\cdots, d_H(C_6)\}$.

We will show that the dual code $C^\perp$ of a code C over R is completely characterized by its associated codes $C_j^\perp$ for $j=1,2,3,4,5,6$.

Theorem 2.1　Let C, expressed as Eq.(1), be a linear code of length n over R, then

$$C^\perp=\eta_1C_1^\perp\oplus\eta_2C_2^\perp\oplus\eta_3C_3^\perp\oplus\eta_4C_4^\perp\oplus\eta_5C_5^\perp\oplus\eta_6C_6^\perp.$$

Moreover, C is self-dual if and only if C_j ($j=1,2,\cdots,6$) are all self-dual over $\mathbb{F}_q$.

Example 2.1　Let C be a linear code of length 6 generated by the matrix G over $R=\mathbb{F}_5+u\mathbb{F}_5+v\mathbb{F}_5+uv\mathbb{F}_5+v^2\mathbb{F}_5+uv^2\mathbb{F}_5$, where

$$G=\begin{pmatrix}\eta_1G_1\\ \eta_2G_2\\ \vdots\\ \eta_6G_6\end{pmatrix},$$

and

$$G_1=\begin{pmatrix}1&2&0&0&0&0\\0&0&1&2&0&0\\0&0&0&0&1&2\end{pmatrix},$$

$$G_2=\begin{pmatrix}1&0&0&2&0&0\\0&1&0&0&2&0\\0&0&1&0&0&3\end{pmatrix},$$

$$G_3=\begin{pmatrix}1&0&0&1&2&2\\0&1&0&2&1&3\\0&0&1&2&3&1\end{pmatrix},$$

$$G_4=\begin{pmatrix}1&3&0&0&0&0\\0&0&1&3&0&0\\0&0&0&0&1&3\end{pmatrix},$$

$$G_5=\begin{pmatrix}1&0&0&1&3&3\\0&1&0&3&1&3\\0&0&1&3&3&1\end{pmatrix},$$

$$G_6=\begin{pmatrix}1&0&0&2&0&0\\0&1&0&0&3&0\\0&0&1&0&0&3\end{pmatrix}.$$

Then C is a self-dual code over R. Moreover, by Theorem 1.1, $\Phi(C)$ is a self-dual code over $\mathbb{F}_5$ with parameters $[36,18,2]$.

3　Skew cyclic codes over R

In the present section, we investigate the structural properties of skew cyclic codes over R with automorphism θ_i. In the commutative case, if $(n,q)=1$, then every cyclic code of length n over $\mathbb{F}_q$ has a unique idempotent generator. However, the skew polynomial ring $\mathbb{F}_q[x,\theta_i]$ does not need to be a unique factorization ring. Note that if $(n, t_i)=1$, then the factorization of x^n-1 in $\mathbb{F}_q[x, \theta_i]$ is unique, where t_i denotes the order of the automorphism θ_i (see Ref.[9]). Now, we give the concept of skew cyclic codes over R.

Definition 3.1　Let R be a ring and θ_i be an automorphism of R. A linear code C of length n over R is a skew cyclic code with the property that

$$c=(c_0,c_1,\cdots,c_{n-1})\in C\Rightarrow$$
$$\sigma(c)=(\theta_i(c_{n-1}),\theta_i(c_0),\cdots,\theta_i(c_{n-2}))\in C,$$

where $\sigma(c)$ is a skew cyclic shift of c.

The skew polynomial representation of a code C is defined to be $\{c_0+c_1x+\cdots+c_{n-1}x^{n-1}\mid(c_0, c_1,\cdots,c_{n-1})\in C\}$. For the sake of convenience, it will be regarded as C itself. The necessary and sufficient conditions for a linear code to be a skew cyclic code are given as follows.

Lemma 3.1[12] A linear code of length n over $\mathbb{F}_q$ is a skew cyclic code with respect to automorphism θ if and only if it is a left $\mathbb{F}_q[x,\theta]$-submodule of $\mathbb{F}_q[x,\theta]/(x^n-1)$. Moreover, if C is a left submodule of $\mathbb{F}_q[x,\theta]/(x^n-1)$, then C is generated by a monic polynomial $g(x)$ which is a right divisor of x^n-1 in $\mathbb{F}_q[x,\theta]$.

We will show that a skew cyclic code over R is completely characterized by its associated codes C_j for $j=1,2,3,4,5,6$, and vice versa.

Theorem 3.1 Let C be a linear code over R of length n and $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, where C_1, C_2, C_3, C_4, C_5 and C_6 are all linear codes of length n over $\mathbb{F}_q$, then C is a skew cyclic code with respect to the automorphism θ_i if and only if C_1, C_2, C_3, C_4, C_5 and C_6 are skew cyclic codes over $\mathbb{F}_q$ with respect to the automorphism θ_i.

Proof For simplicity, the vector $(x^1, x^2, \cdots, x^n)$ $((x_v^1, x_v^2, \cdots, x_v^n), \sim v\in\backslash\mathbb{Z})$ denotes the codeword of a code of length n.

Let $(x_j^1, x_j^2, \cdots, x_j^n)\in C_j$ for $j=1,2,3,4,5,6$. Assume that $x^i=\sum_{j=1}^{6}\eta_j x_j{}^i$ for $i=1,2,\cdots,n$, then the vector $x=(x^1,x^2,\cdots,x^n)\in C$. If C is a skew cyclic code, then $(\theta_i(x^n),\theta_i(x^1),\cdots,\theta_i(x^{n-1}))\in C$. Note that $\sigma(x)=(\theta_i(x^n),\theta_i(x^1),\cdots,\theta_i(x^{n-1}))=\sum_{j=1}^{6}\eta_j((x_j^n)^{p^i},(x_j^1)^{p^i},\cdots,(x_j{}^{n-1})^{p^i})$. So $(\theta_i(x_j^n),\theta_i(x_j^1),\cdots,\theta_i(x_j{}^{n-1}))=((x_j^n)^{p^i},(x_j^1)^{p^i},\cdots,(x_j{}^{n-1})^{p^i})\in C_j$, which implies that C_j are all skew cyclic codes over $\mathbb{F}_q$ for $j=1,2,3,4,5,6$.

On the other hand, suppose that C_j are all skew cyclic codes over $\mathbb{F}_q$ for $j=1,2,3,4,5,6$, and $y=(y^1,y^2,\cdots,y^n)\in C$, where $y^i=\sum_{j=1}^{6}\eta_j y_j{}^i$ for $i=1,2,\cdots,n$, then $(y_j^1,y_j^2,\cdots,y_j^n)\in C_j$ for $j=1,2,\cdots,6$. Note that $(\theta_i(y_j^n),\theta_i(y_j^1),\cdots,\theta_i(y_j{}^{n-1}))=((y_j^n)^{p^i},(y_j^1)^{p^i},\cdots,(y_j{}^{n-1})^{p^i})\in C_j$ for $j=1,2,\cdots,6$. Thus $\sigma(y)=(\theta_i(y^n),\theta_i(y^1),\cdots,\theta_i(y^{n-1}))=\sum_{j=1}^{6}\eta_j((y_j^n)^{p^i},(y_j^1)^{p^i},\cdots,(y_j{}^{n-1})^{p^i})\in\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6=C$. Therefore C is a skew cyclic code over R.

In view of the previous theorem, the following corollary can be easily obtained.

Corollary 3.1 If C is a skew cyclic code over R, then the dual code $C^\perp$ is also skew cyclic.

Proof By Theorem 2.1, we have $C^\perp=\eta_1C_1^\perp\oplus\eta_2C_2^\perp\oplus\eta_3C_3^\perp\oplus\eta_4C_4^\perp\oplus\eta_5C_5^\perp\oplus\eta_6C_6^\perp$. According to Corollary 18 in Ref.[2], we know that the dual code of every skew cyclic code over $\mathbb{F}_q$ is also skew cyclic. Hence the dual code $C^\perp$ is a skew cyclic code from Theorem 3.1.

Next, we give the definition of skew quasi cyclic codes over R.

Definition 3.2 Let C be a linear code of length n over $\mathbb{F}_q$ and $(c^1|c^2|\cdots|c^l)$ be a codeword in C divided into l equal parts of length s where $n=sl$. If $(\sigma(c^1)|\sigma(c^2)|\cdots|\sigma(c^l))\in C$, then the linear code C which is permutation equivalent to C is called a skew quasi cyclic code of index l or skew l-quasi cyclic code.

Based on the definition of skew quasi cyclic codes, we have the following corollary.

Corollary 3.2 If C is a skew cyclic code of length n over R, then $\Phi(C)$ is a skew 6-quasi cyclic code of length $6n$ over $\mathbb{F}_q$.

Proof The result follows from the Definition 3.2 and the definition of Gray map Φ.

We are now ready to consider the generator polynomial of a skew cyclic code of length n over R.

Theorem 3.2 Let $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_1C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$ be a skew cyclic code of length n over R and assume that $C_j=\langle g_j(x)\rangle$ for $j=1,2,3,4,5,6$, then $C=\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ and $|C|=q^{6n-\sum_{j=1}^{6}\deg(g_j(x))}$.

Proof For the sake of convenience, we denote the ideal $\langle\eta_1g_1(x),\eta_2g_2(x),\eta_3g_3(x),\eta_4g_4(x),\eta_5g_5(x),\eta_6g_6(x)\rangle$ by I. In the following, we prove $C=I$. Since $C_j=\langle g_j(x)\rangle$, $|C_j|=q^{n-\deg(g_j(x))}$, $j=1,2,3,4,5,6$, and $C=\eta_1C_1\oplus\eta_2C_2\oplus\eta_3C_3\oplus\eta_4C_4\oplus\eta_5C_5\oplus\eta_6C_6$, then $C=\left\{\sum_{j=1}^{6}\eta_jk_j(x)g_j(x)\mid k_j(x)\in\mathbb{F}_q[x,\theta],1\leqslant j\leqslant 6\right\}$.