(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 105680992 B
(45)授权公告日 2019.05.03

(21)申请号 201610051144.9

(22)申请日 2016.01.26

(65)同一申请的已公布的文献号
申请公布号 CN 105680992 A

(43)申请公布日 2016.06.15

(73)专利权人 华中科技大学
地址 430074 湖北省武汉市洪山区珞喻路1037号

(72)发明人 彭立 李高峰 魏蛟龙 梁琨 周波

(74)专利代理机构 华中科技大学专利中心 42201
代理人 曹葆青

(51)Int.Cl.
H04L 1/00(2006.01)

(56)对比文件
CN 1461530 A,2003.12.10,
CN 101385245 A,2009.03.11,
EP 1463255 A1,2004.09.29,
CN 104836634 A,2015.08.12,
Stergios Stergiou.Implicit Permutation Enumeration Networks and Binary Decision Diagrams Reordering.《IEEE》.2011,

审查员 黄睿

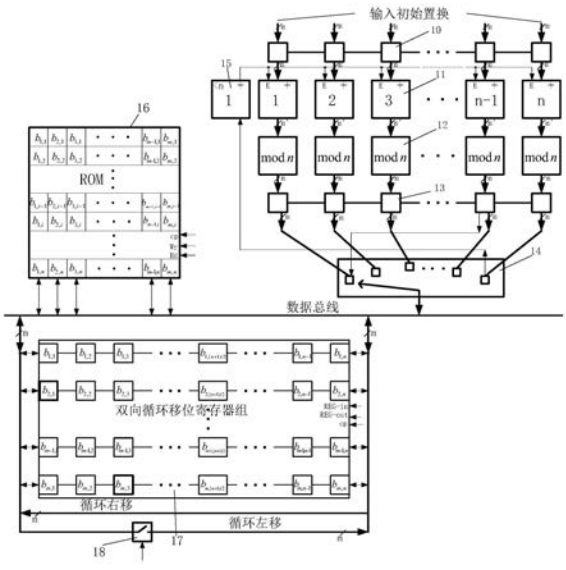
权利要求书3页 说明书10页 附图3页

(54)发明名称

一种通信信道编码方法及置换码集合产生器

(57)摘要

本发明公开一种通信置换调制方法及置换码集合产生器。所述陪集划分(n,n(n-1),n-1)置换群码具有纠错能力d-1,对混合多频率噪声和信号衰落同时发生的信道干扰具有较强的抑制能力。所述陪集划分(n,n(n-1),n-1)置换群码的构造方法是指码长n为素数时,针对最小距离为n-1码集合尺寸为n(n-1)的置换码家族,提出首先用$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$计算n-1个轨道首置换码字、然后用$P_n=C_n0_n=\{(1_1)^{n-1}0_n\}=\{(r_n)^{n-1}0_n\}$枚举码集合中其余码字的构造方法。本发明还提供了相应的(n,n(n-1),n-1)置换群码的码集合产生器。本发明所提出的陪集划分(n,n(n-1),n-1)置换群码是一类代数结构码,轨道首阵列中的n-1个码字可以用简单的加法器和(mod n)计算器来取代正整数的乘法运算;用良好定义的循环移位复合操作函数来取代循环子群对轨道首置换的合成运算,采用循环移位寄存器组来实现循环群对置换的操作。



CN 105680992 B

1.一种通信信道编码方法,包括陪集划分(n,n(n-1),n-1)置换群码的构造步骤,其特征在于:置换群码的构造步骤具体为:

码长为n最小距离为n-1码集合尺寸为n(n-1)的置换群码的结构为$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=C_nO_n=\{\{C_no_1\},\{C_no_2\},...,\{C_no_{n-1}\}\}=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}$;所述码集合$P_n=C_nO_n$是以循环置换子群$C_n$和与循环置换子群$C_n$不相同的另一个子群$O_n$互为陪集的置换群码;$p_{\beta\alpha}$为码集合$P_n$中的每一个置换码字;

循环置换子群$C_n=\{\gamma\pi\}=\{<\gamma_2>[a_1a_2...a_n]\}$,规定$\gamma=\{\gamma_1,\gamma_2,...,\gamma_n\}$的每一个下标值与$C_n$中每一个置换的第一个元素的下标值保持一致,即$c_1=\gamma_1\pi=c_2^n=\gamma_2^n\pi=(a_2a_3...a_na_1)^n[a_1a_2...a_n]=[a_1a_2...a_n]$,$c_2=\gamma_2\pi=[a_2a_3...a_na_1]$,$c_3=\gamma_3\pi=c_2^2=\gamma_2^2\pi=(a_2a_3...a_na_1)^2[a_1a_2...a_n]=[a_3a_4...a_na_1a_2]$,…,$c_n=\gamma_n\pi=c_2^{n-1}=\gamma_2^{n-1}\pi=(a_2a_3...a_na_1)^{n-1}[a_1a_2...a_n]=[a_na_1a_2...a_{n-1}]$,那么$C_n$的最小距离是$d_{Cn}=n$,它的势是$|C_n|=n$,$(a_1a_2...a_n)$表示置换算子;

子群O_n是(n-1)×n的置换阵列或是n-1个置换构成的集合,$O_n=\{o_\alpha\}_{\alpha=1}^{n-1}=\{\alpha\cdot o_1\}_{\alpha=1}^{n-1}$,其中$o_1=[12...n]$是单位置换,$\alpha=1,2,...,n-1$是置换阵列$O_n$的行号;

所述码集合$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}$中的每一个置换码字$p\beta\alpha$由循环置换子群$C_n$中的置换$c_\beta$与子群$O_n$中的置换$o_\alpha$的合成运算产生,$\alpha=1,2,...n-1$和$\beta=1,2,...n$。

2.根据权利要求1所述的通信信道编码方法,其特征在于,用循环左移复合操作函数$(l_1)^{n-1}$或循环右移复合操作函数$(r_n)^{n-1}$取代C_n,将两个置换子群C_n和O_n的合成运算转换为硬件可执行的循环移位操作;所述用$(l_1)^{n-1}$或$(r_n)^{n-1}$取代C_n的操作,具体为:置换群中的每个轨道$\{C_no_\alpha\}$用其等效表达式$\{C_no_\alpha\}=\{(r_n)^{n-1}o_\alpha\}=\{(l_1)^{n-1}o_\alpha\}$来执行,$\alpha=1,2,...n-1$;所述码集合$P_n=C_nO_n$用其等效表达式$P_n=C_nO_n=\{(r_n)^{n-1}O_n\}=\{\{(r_n)^{n-1}o_1\},\{(r_n)^{n-1}o_2\},...,\{(r_n)^{n-1}o_{n-1}\}\}$或$P_n=C_nO_n=\{(l_1)^{n-1}O_n\}=\{\{(l_1)^{n-1}o_1\},\{(l_1)^{n-1}o_2\},...,\{(l_1)^{n-1}o_{n-1}\}\}$来执行;

循环左移复合操作函数$(l_1)^{n-1}$或循环右移复合操作函数$(r_n)^{n-1}$表示为:构造循环左移复合操作函数$f_{CF-l}(n-1,\Lambda)=\underbrace{l_1l_1...l_1}_{n-1}=(l_1)^{n-1}$,$l_1\pi=l_1[a_1a_2...a_n]=[a_2a_3...a_{n-1}a_na_1]$,称$l_1$是一个置换的循环左移操作函数,构造循环右移复合操作函数$f_{CF-r}(n-1,\Lambda)=\underbrace{r_nr_n...r_n}_{n-1}=(r_n)^{n-1}$,$r_n\pi=r_n[a_1a_2...a_n]=[a_na_1a_2...a_{n-1}]$,称$r_n$是一个置换的循环右移操作函数,$f_{CF}(u,\Lambda)$为将左移操作函数集$T_{left}$或者右移操作函数集$T_{right}$集合中部分或全部操作函数排列成串或者排列成不同函数幂的连乘,那么这些操作函数串或操作函数幂的积将形成复合操作函数。

3.根据权利要求1所述的通信信道编码方法,其特征在于,所述置换子群O_n等效为轨道首阵列,其构造方法具体为:

如果置换中包含0元素,用O_{n1}表示置换子群O_n:则设$a_{\alpha_1,\beta_1}\in Z_n^0=\{0,1,...,n-1\}$表示阵列$O_{n1}$中第$\alpha_1$行第$\beta_1$列的一个元素,其中$\alpha_1=0,1,...,n-2$表示阵列$O_{n1}$的行索引,$\beta_1=0,1,...,n-1$表示阵列$O_{n1}$的列索引,$k_1=0,1,...,n-1$表示$O_{n1}$中第$k_1$列是与$k_1$相同的元素;当n是素数时,且$a_{\alpha_1,\beta_1}$是n的倍数xn,规定$a_{\alpha_1,\beta_1}=0$,x是任意整数;轨道首阵列$O_{n1}$中每一个置换的每一个元

素的计算表达式为$a_{\alpha_1,\beta_1}(k_1)=[(\alpha_1+1)\times(\beta_1-k_1)+k_1](\mathrm{mod}\,n)$，轨道首阵列的n-1个置换的计算表达式为$O_{n1}(k_1)=\{o_0,o_1,...,o_{n-2}\}=\{\{a_{\alpha_1,\beta_1}(k_1)\}_{\alpha_1=0}^{n-2}\}_{\beta_1=0}^{n-1}$，其中$k_1=0,1,...,n-1$；或者，

如果置换中不包含0元素，用0_{n2}表示置换子群0_n：设$a_{\alpha_2,\beta_2}\in Z_n^1=\{1,2,...,n\}$表示阵列$0_{n2}$中第$\alpha_2$行第$\beta_2$列的一个元素，其中$\alpha_2=1,2,...,n-1$表示阵列$0_{n2}$的行索引，$\beta_2=1,2,...,n$表示阵列$0_{n2}$的列索引，$k_2=1,2,...,n$表示$0_{n2}$中第$k_2$列是与$k_2$相同的元素；当n是素数时，且$a_{\alpha_2,\beta_2}$是n的倍数xn，规定$a_{\alpha_2,\beta_2}=n$，x是任意整数；轨道首阵列$0_{n2}$中每一个置换的每一个元素的计算表达式为$a_{\alpha_2,\beta_2}(k_2)=[\alpha_2(\beta_2-k_2)+k_2](\mathrm{mod}\,n)$，轨道首阵列的n-1个置换的计算表达式为$O_{n2}(k_2)=\{o_1,o_2,...,o_{n-1}\}=\{\{a_{\alpha_2,\beta_2}(k_2)\}_{\alpha_2=1}^{n-1}\}_{\beta_2=1}^{n}$，其中$k_2=1,2,...,n$；设$k_2=n$和$a_{\alpha,\beta}\in Z_n^1=\{1,2,...,n\}$，所述轨道首阵列$0_{n2}$中每一个置换的每一个元素的计算表达式简化为$a_{\alpha,\beta}(n)=[\alpha\cdot\beta](\mathrm{mod}\,n)$，轨道首阵列$0_{n2}$的n-1个置换的计算表达式简化为$O_{n2}=\{o_1,o_2,...,o_{n-1}\}=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$，其中$o_1=e=[a_1a_2...a_n]=[12...n]$，$a_1,a_2,...,a_n\in Z_n^1$，$\alpha=1,2,...n-1$和$\beta=1,2,...n$。

4.一种陪集划分(n,n(n-1),n-1)置换群码的码集合产生器，其特征在于，包括轨道首阵列产生器、ROM存储器和双向循环移位寄存器组，其中：

所述轨道首阵列产生器用于执行置换子群$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$的计算，产生n-1个轨道首置换，$\alpha=1,2,...n-1$，码长为n，$o_1$为初始置换；

所述ROM存储器存储轨道首阵列产生器的输出结果和双向循环移位寄存器组的输出结果；

所述双向循环移位寄存器组对一个置换执行循环左移复合操作函数$(l_1)^{n-1}$或者循环右移复合操作函数$(r_n)^{n-1}$的操作，实现每个轨道首置换o_α的轨道$\{(l_1)^{n-1}o_\alpha\}$或者$\{(r_n)^{n-1}o_\alpha\}$的计算和码集合$\{(l_1)^{n-1}0_n\}$或者$\{(r_n)^{n-1}0_n\}$的计算；循环左移复合操作函数$(l_1)^{n-1}$或循环右移复合操作函数$(r_n)^{n-1}$表示为：构造循环左移复合操作函数$f_{CF-l}(n-1,\Lambda)=\underbrace{l_1l_1...l_1}_{n-1}=(l_1)^{n-1}$，$l_1\pi=l_1[a_1a_2...a_n]=[a_2a_3...a_{n-1}a_na_1]$，称$l_1$是一个置换的循环左移操作函数，构造循环右移复合操作函数$f_{CF-r}(n-1,\Lambda)=\underbrace{r_nr_n...r_n}_{n-1}=(r_n)^{n-1}$，$r_n\pi=r_n[a_1a_2...a_n]=[a_na_1a_2...a_{n-1}]$，称$r_n$是一个置换的循环右移操作函数，$f_{CF}(u,\Lambda)$为将左移操作函数集$T_{left}$或者右移操作函数集$T_{right}$集合中部分或全部操作函数排列成串或者排列成不同函数幂的连乘，那么这些操作函数串或操作函数幂的积将形成复合操作函数；

所述轨道首阵列产生器用于在输入初始置换是单位置换$o_1=e=[12...n]$的条件下，执行n-1个轨道首置换$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)=\{o_1,2o_1,...,(n-1)o_1\}(\mathrm{mod}\,n)$的计算，并将n-1个轨道首置换存入ROM存储器中；所述轨道首阵列产生器包括n个并行运行输入缓存器、n个并行运行正整数加法器、n个并行运行modn计算器、n个并行运行输出缓存器、n输入单输出开关和使能信号产生器，其中：

所述n个并行运行输入缓存器由n个m位二进制的寄存器构成，每一个寄存器的输入端和输出端分别连接m根并行数据线，m满足$2^{m-1}+1\leqslant n\leqslant 2^m$；

所述n个并行运行正整数加法器执行$\{\alpha o_1\}_{\alpha=1}^{n-1}$运算，每一个正整数加法器由m'个二进制全加器和m'位B寄存器构成，$m<m'\leq\lceil\log_2(n-1)^2\rceil$，m根数据线并行输入，m'根数据线并行输出；所述二进制全加器的一个输入端接收输入缓存器的数据，另一个输入端与B寄存器的输出端相连，二进制全加器的输出端与B寄存器的输入端相连；使能信号E＝1时，所述n个并行运行正整数加法器工作，E＝0时，其不工作；

所述n个并行运行modn计算器用于完成$\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$计算，每个modn计算器由一个两输入端单输出端通用modn计算器、m位C寄存器和m位D寄存器构成，m'根数据线并行输入，m根数据线并行输出；所述通用modn计算器的一个输入端有m'根并行输入数据线与所述n个并行运行正整数加法器中m'位B寄存器的输出端相连，另一个输入端有m根并行输入数据线与m位C寄存器的输出端相连；所述通用modn计算器的输出端有m根并行输出数据线；所述m位C寄存器存储数据n所对应的m位二进制值，并保持不变；所述m位D寄存器存储通用modn计算器的输出值，如果D寄存器的值不为0，则将D寄存器的值作为输出值，否则输出C寄存器的值；

所述n个并行运行输出缓存器由n个m位的寄存器构成，每一个寄存器的输入端和输出端分别连接m根并行数据线；所述n个并行运行输出缓存器的第n-1个缓存器准备好当前数据时，发出信号使所述n输入单输出开关的第一个开关闭合；

所述n输入单输出开关用于将所述n个并行运行输出缓存器的n个数据的每一个串行输出到总线上，从1到n每接通一个开关，每一个输出缓存器的m根数据线与m根并行总线接通；所述n输入单输出开关的第一个开关闭合的信号来自所述n个并行运行输出缓存器的第n-1个缓存器所发出的控制信号；所述n输入单输出开关的第n个开关闭合时，输出一个高电平信号至使能信号产生器的输入端；

所述使能信号产生器为所述n个并行运行正整数加法器提供使能信号，它由二进制加1计数器和单稳态触发器构成，一根输入信号线，一根输出信号线，常态输出低电平；所述二进制加1计数器的输入端与所述n输入单输出开关的第n个开关的输出信号线相连，当收到输入控制信号时，所述二进制加1计数器做一次加1操作，并使单稳态触发器产生持续时间为1个cp的高电平脉冲，通过一根信号线输出到所述n个并行运行正整数加法器的E信号端；二进制加1计数器加n-1次，所述单稳态触发器不发脉冲信号，所述使能信号产生器输出低电平。

5.根据权利要求4所述陪集划分(n,n(n-1),n-1)置换群码的码集合产生器，其特征在于，所述双向循环移位寄存器组用于轨道$\{(l_1)^{n-1}o_\alpha\}$与$\{(r_n)^{n-1}o_\alpha\}$的实现，以及码集合$\{(l_1)^{n-1}0_n\}$与$\{(r_n)^{n-1}0_n\}$的实现；所述双向循环移位寄存器组的结构是由m行n列的触发器阵列构成，每一行由n个触发器形成既能循环左移又能循环右移的双向移位寄存器；在循环左移回路的每一个回路中串接一个开关，m个开关并行运行，m个开关闭合，则执行m个数据并行的循环左移操作，m个开关断开，则执行m个数据并行的左移输入和左移输出操作；设置两个控制信号输入端REG-in和REG-out，可以组合四种控制信号00,01,10,11，分别对应双向循环移位寄存器组的四种工作状态：左移输入，左移输出，循环左移和循环右移。

一种通信信道编码方法及置换码集合产生器

技术领域

[0001] 本发明属于通信传输中的信道编码技术领域，更具体地，涉及一种通信置换调制方法及陪集划分(n,n(n-1),n-1)置换码集合产生器的构造方法及其码集合产生器。

背景技术

[0002] 在电力线信道上存在多径衰落、窄带永久噪声、宽带脉冲噪声和有色背景噪声等多种干扰并存或同时出现的情况，像这样多种干扰同时发生的情况很少在无线和有线信道上出现，由此可以推知如果将现有无线和有线通信的成熟技术直接搬移到电力线载波通信信道上，信息传输的可靠性很难得到保证。从这个角度讲，有必要对电力线载波通信中多种形式、多频率干扰问题提出可靠性要求更高的纠错码解决方案。除了电力线载波信道外，其它存在多种形式和多种频率干扰同时发生的无线和有线信道，也需要使用更高可靠性的纠错码方案。

[0003] 2000年Vinck将置换码引入到电力线载波通信中，发表“‘Coded modulation for powerline communications’,AEU int.J.Electron.Commun.,vol.54,no.1,pp:45-49,2000”一文，提出将M维FSK调制与置换码相结合的电力线载波编码调制解决方案。该方案在发射机端，利用置换码的非线性冗余同时引入了时间分集和频率分集，增强了抵抗多频率和衰落干扰的能力；在接收机端，可以采用常包络解调算法对接收信号进行检测，自然形成简单的非相干解调方案。特别值得关注的是Vinck分析了一组码长为4的置换码，得出特殊结构的置换码具有纠错能力d-1而不是$\lfloor (d-1)/2 \rfloor$的结论。然而，Vinck并没有给出有效的置换码构造方法，目前关于纠错能力为d-1的置换码并没有得到实际应用，其发展缓慢的关键原因是置换码的代数结构设计方法较少，特别是硬件可执行方案还没有得到有效解决。

发明内容

[0004] 本发明提出一种用于通信调制的陪集划分(n,n(n-1),n-1)置换群码的构造方法及其码集合产生器，具体为一种码长n、最小距离n-1、码字数量n(n-1)、纠错能力d-1＝n-2的置换码代数结构设计方法和码字枚举器。针对电力线载波通信中的多径衰落、窄带永久噪声、宽带脉冲噪声和有色背景噪声等多种干扰并存或同时出现的情况，本发明提供一种有效抵抗这些组合干扰的高可靠性的纠错码设计方案。此外，针对无线通信中的多频率干扰，以及人为恶意频率干扰，本发明所提出的置换群码也具有较强的抑制能力。总之，在数据传输率要求不高但各种混合频率干扰和深度衰落同时存在的运行环境中，本发明所提出的陪集划分(n,n(n-1),n-1)置换群码对所传输的信号均具有保护能力。

[0005] 为了实现上述目的，按照本发明的一个方面，提供了一种陪集划分(n,n(n-1),n-1)置换群码的构造方法，码长为n最小距离为n-1码集合尺寸为n(n-1)的置换群码的结构为$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=C_nO_n=\{\{C_no_1\},\{C_no_2\},...,\{C_no_{n-1}\}\}=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}$；所述码集合$P_n$＝$C_nO_n$是以循环置换子群$C_n$和不相同的另一个子群$O_n$互为陪集；所述码集合$P_n$＝{$\{C_no_1\}$,$\{C_no_2\}$,...,$\{C_no_{n-1}\}$}是置换子群$C_n$将$P_n$划分成n-1个陪集，每一个陪集$\{C_no_\alpha\}$形成一个置换

o_α的轨道或循环拉丁方(C-LS)；所述码集合$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}$是每一个置换码字$p_{\beta\alpha}$由子群$C_n$中的置换$c_\beta$与子群$O_n$中的置换$o_\alpha$的合成运算产生，$\alpha=1,2,...n-1$和$\beta=1,2,...n$。

[0006] 按照本发明的另一方面，还提供了一种陪集划分(n,n(n-1),n-1)置换群码的码集合产生器，包括轨道首阵列产生器、ROM存储器和双向循环移位寄存器组，其中：

[0007] 所述轨道首阵列产生器用于执行$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$计算，产生n-1个轨道首置换；

[0008] 所述ROM存储器存储轨道首阵列产生器的输出结果和双向循环移位寄存器组的输出结果；

[0009] 所述双向循环移位寄存器组执行$(l_1)^{n-1}$或者$(r_n)^{n-1}$对一个置换的操作，实现每个轨道首置换o_α的轨道$\{(l_1)^{n-1}o_\alpha\}$或者$\{(r_n)^{n-1}o_\alpha\}$的计算和码集合$\{(l_1)^{n-1}O_n\}$或者$\{(r_n)^{n-1}O_n\}$的计算，$\alpha=1,2,...,n-1$。

[0010] 有益效果：本发明所提出的陪集划分(n,n(n-1),n-1)置换群码是一类代数结构码，码集合中的轨道首置换码字可以用简单的加法运算和(modn)运算完成，不需要进行复杂的合成运算，整个码集合可以用循环移位寄存器硬件实现；作为多进制纠错码类，其纠错能力为d-1是传统多进制纠错码类纠错能力$\lfloor (d-1)/2 \rfloor$的两倍；当与MFSK调制技术结合时，接收机端能够采用简单的非相干常包络解调技术进行解调；对在混合多频率噪声和深度衰落同时存在的干扰信道上，信号传输的可靠性能够得到保证。

附图说明

[0011] 图1为本发明中(n,n(n-1),n-1)置换群码发生器电路总体框图；

[0012] 图2为本发明中轨道首阵列产生电路示意图；

[0013] 图3为本发明中ROM存储器示意图；

[0014] 图4为本发明中n进制双向循环移位寄存器组示意图。

具体实施方式

[0015] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。此外，下面所描述的本发明各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0016] 基本原理

[0017] 这一部分描述本发明所涉及的陪集划分(n,n(n-1),n-1)置换群码的基本原理。

[0018] 编码的符号可在两个有限域中取值，即设$Z_n^0=\{0,1,...,n-1\}$是包含0元素的n阶有限域，设$Z_n^1=\{1,2,...,n\}$是不包含0元素的n阶有限正整数域，也是一个阶为n的循环群。定义在Z_n^0或Z_n^1上的n个元素的所有n!个置换所形成的集合称为对称群，用$S_n=\{\pi_1,...,\pi_k,...,\pi_{n!}\}$表示，其中每个元素可用一个置换$\pi_k=[a_1...a_i...a_n]$来表示，每个置换的元素为$a_1...a_i...a_n\in Z_n^0$或$a_1...a_i...a_n\in Z_n^1$，每个置换的度(维数)为$|\pi_k|=n$，对称群的势(阶)为$|S_n|=$

n!。设π_0=e=[$a_1a_2...a_n$]=[01...n-1]或π_0=e=[$a_1a_2...a_n$]=[12...n]表示对称群S_n的单位元。[$a_1a_2...a_n$]表示S_n中的置换，($a_1a_2...a_n$)表示置换算子。

[0019] 如果群$H \subset S_n$是由单一元素产生，即存在元素x∈H以至于在合成运算下有$H=\{x^i \mid i \in Z_n^1, x, x^i \in S_n\}$，那么H是一个循环置换群，表示成H=<x>，并且称H是由x产生的，或者x是H的生成子。

[0020] 假设γ=<γ_2>是由n个置换算子构成的循环置换群，其生成子γ_2=($a_2a_3...a_na_1$)，它的势是|γ|=n。如果使算子集合γ=<γ_2>作用于一个置换π=[$a_1...a_i...a_n$]，得到$\{\gamma\pi\}=\{\{\gamma_2,\gamma_3,...,\gamma_n,\gamma_1\}[a_1...a_i...a_n]\}=\{\langle\gamma_2\rangle\pi\}=\{\{\gamma_2,\gamma_2^2,...,\gamma_2^{n-1},\gamma_2^n\}[a_1...a_i...a_n]\}$，那么称{$\gamma\pi$}是在循环群$\gamma$作用下包含置换$\pi$的一个轨道，并且这个轨道所包含的元素的数量是|{$\gamma\pi$}|=n。

[0021] 下面的三个定理或引理未加证明地提供了陪集划分(n,n(n-1),n-1)置换群码的基本结构。

[0022] 引理1[循环群C_n的结构]：设C_n={$\gamma\pi$}={<γ_2>[$a_1a_2...a_n$]}，规定γ={γ_1,γ_2,...,γ_n}的每一个下标值与C_n中每一个置换的第一个元素的下标值保持一致，即$c_1=\gamma_1\pi=c_2^n=\gamma_2^n\pi=(a_2a_3...a_na_1)^n[a_1a_2...a_n]=[a_1a_2...a_n]$，$c_2=\gamma_2\pi=[a_2a_3...a_na_1]$，$c_3=\gamma_3\pi=c_2^2=\gamma_2^2\pi=(a_2a_3...a_na_1)^2[a_1a_2...a_n]=[a_3a_4...a_na_1a_2]$，…，$c_n=\gamma_n\pi=c_2^{n-1}=\gamma_2^{n-1}\pi=(a_2a_3...a_na_1)^{n-1}[a_1a_2...a_n]=[a_na_1a_2...a_{n-1}]$，那么$C_n$={$c_1,c_2,...,c_n$}=<$c_2$>={<$\gamma_2$>$\pi$}是$S_n$的子群，也是一个循环置换群，它的最小距离是$d_{C_n}=n$，它的势是|$C_n$|=n。

[0023] 定理2[O_n的结构]：设O_n是(n-1)×n的置换阵列或是n-1个置换构成的集合，构造$O_n=\{o_\alpha\}_{\alpha=1}^{n-1}=\{\alpha\cdot o_1\}_{\alpha=1}^{n-1}$，其中$o_1$=[12...n]是单位置换，$\alpha$=1,2,...,n-1是置换阵列$O_n$的行号，也是集合$O_n$所包含的置换数量的索引。当且仅当1)n是素数；2)对所有的α=1,2,...,n-1，有(α•n)(modn)=n；那么集合O_n是S_n的子群，阵列O_n的第n列全为n，并且O_n的最小距离是$d_{O_n}=n-1$，它的势是|O_n|=n-1。

[0024] 定理3[由C_n和O_n构造置换群码P_n]：对任意素数n，设P_n={p_{11},...,$p_{\beta\alpha}$,...,$p_{n(n-1)}$}是S_n的非平凡子群。用C_n和O_n的合成来构造P_n，即有$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=C_nO_n=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}$，其中$c_\beta\circ o_\alpha$表示置换$c_\beta$和置换$o_\alpha$的合成运算。如果$C_n\cap O_n$=e=[12...n]，那么$P_n$是以$C_n$和$O_n$互为陪集的置换群码，$P_n$的最小汉明距离是$d_{P_n}=n-1$，它的势是|$P_n$|=n(n-1)。

[0025] 例1：设n=5，根据引理1得到下列C_5，

[0026]

$$C_5=\begin{Bmatrix}c_1,\\c_2,\\c_3,\\c_4,\\c_5\end{Bmatrix}=\langle c_2\rangle=\begin{Bmatrix}c_2^5,\\c_2^1,\\c_2^2,\\c_2^3,\\c_2^4\end{Bmatrix}=\langle\gamma_2\pi\rangle=\begin{Bmatrix}\gamma_2^5\pi,\\\gamma_2^1\pi,\\\gamma_2^2\pi,\\\gamma_2^3\pi,\\\gamma_2^4\pi\end{Bmatrix}=\begin{Bmatrix}(a_2a_3a_4a_5a_1)^5[a_1a_2a_3a_4a_5],\\(a_2a_3a_4a_5a_1)[a_1a_2a_3a_4a_5],\\(a_2a_3a_4a_5a_1)^2[a_1a_2a_3a_4a_5],\\(a_2a_3a_4a_5a_1)^3[a_1a_2a_3a_4a_5],\\(a_2a_3a_4a_5a_1)^4[a_1a_2a_3a_4a_5]\end{Bmatrix}=\begin{Bmatrix}a_1a_2a_3a_4a_5,\\a_2a_3a_4a_5a_1,\\a_3a_4a_5a_1a_2,\\a_4a_5a_1a_2a_3,\\a_5a_1a_2a_3a_4,\end{Bmatrix}=\begin{Bmatrix}12345,\\23451,\\34512,\\45123,\\51234\end{Bmatrix}$$

[0027] 根据定理2得到下列O_5的置换阵列形式

[0028]

$$O_5=\begin{bmatrix}o_1\\o_2\\o_3\\o_4\end{bmatrix}=\begin{bmatrix}1o_1\\2o_1\\3o_1\\4o_1\end{bmatrix}=\begin{bmatrix}1\cdot1&1\cdot2&1\cdot3&1\cdot4&1\cdot5\\2\cdot1&2\cdot2&2\cdot3&2\cdot4&2\cdot5\\3\cdot1&3\cdot2&3\cdot3&3\cdot4&3\cdot5\\4\cdot1&4\cdot2&4\cdot3&4\cdot4&4\cdot5\end{bmatrix}(\mathrm{mod}\,5)=\begin{bmatrix}1&2&3&4&5\\2&4&6&8&10\\3&6&9&12&15\\4&8&12&16&20\end{bmatrix}(\mathrm{mod}\,5)=\begin{bmatrix}1&2&3&4&5\\2&4&1&3&5\\3&1&4&2&5\\4&3&2&1&5\end{bmatrix}$$

[0029] 那么O_5的集合形式为$O_5=\begin{Bmatrix}o_1,\\o_2,\\o_3,\\o_4\end{Bmatrix}=\begin{Bmatrix}a_1a_2a_3a_4a_5,\\a_2a_4a_1a_3a_5,\\a_3a_1a_4a_2a_5,\\a_4a_3a_2a_1a_5\end{Bmatrix}=\begin{Bmatrix}12345,\\24135,\\31425,\\43215\end{Bmatrix}$,

[0030] 设$c_1=o_1=e=[12345]$,根据定理3得到下列P_5,

[0031]

$$P_5=\{\{p_{\beta\alpha}\}_{\beta=1}^{5}\}_{\alpha=1}^{4}=\{\{C_5o_1\},\{C_5o_2\},\{C_5o_3\},\{C_5o_4\}\}=\{\{c_\beta\circ o_\alpha\}_{\beta=1}^{5}\}_{\alpha=1}^{4}=\begin{Bmatrix}c_1\circ o_1,&c_1\circ o_2,&c_1\circ o_3,&c_1\circ o_4,\\c_2\circ o_1,&c_2\circ o_2,&c_2\circ o_3,&c_2\circ o_4,\\c_3\circ o_1,&c_3\circ o_2,&c_3\circ o_3,&c_3\circ o_4,\\c_4\circ o_1,&c_4\circ o_2,&c_4\circ o_3,&c_4\circ o_4,\\c_5\circ o_1,&c_5\circ o_2,&c_5\circ o_3,&c_5\circ o_4\end{Bmatrix}$$

$$=\begin{Bmatrix}a_1a_2a_3a_4a_5,&a_2a_4a_1a_3a_5,&a_3a_1a_4a_2a_5,&a_4a_3a_2a_1a_5,\\a_2a_3a_4a_5a_1,&a_3a_5a_2a_4a_1,&a_4a_2a_5a_3a_1,&a_5a_4a_3a_2a_1,\\a_3a_4a_5a_1a_2,&a_4a_1a_3a_5a_2,&a_5a_3a_1a_4a_2,&a_1a_5a_4a_3a_2,\\a_4a_5a_1a_2a_3,&a_5a_2a_4a_1a_3,&a_1a_4a_2a_5a_3,&a_2a_1a_5a_4a_3,\\a_5a_1a_2a_3a_4,&a_1a_3a_5a_2a_4,&a_2a_5a_3a_1a_4,&a_3a_2a_1a_5a_4\end{Bmatrix}=\begin{Bmatrix}12345,&24135,&31425,&43215,\\23451,&35241,&42531,&54321,\\34512,&41352,&53142,&15432,\\45123,&52413,&14253,&21543,\\51234,&13524,&25314,&32154\end{Bmatrix}$$

[0032] 例1说明P_5是码长为5,最小距离为4,码字个数为20,纠错能力为3的置换群码。从P_5中可以看出,P_5由4个轨道$\{C_5o_1\}$,$\{C_5o_2\}$,$\{C_5o_3\}$,$\{C_5o_4\}$构成。

[0033] 技术方案

[0034] 技术方案分为两部分。第一部分是基于陪集划分(n,n(n-1),n-1)置换群码的构造方法;第二部分是(n,n(n-1),n-1)置换群码的码集合产生器的结构设计。

[0035] 第一部分:陪集划分(n,n(n-1),n-1)置换群码的构造方法

[0036] 根据引理1、定理2和3,陪集划分(n,n(n-1),n-1)置换群码的构造方法是:码集合中的所有码字由$P_n=\{\{p_{\beta\alpha}\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=C_nO_n=\{\{C_no_1\},\{C_no_2\},\ldots,\{C_no_{n-1}\}\}=\{\{c_\beta\circ o_\alpha\}_{\alpha=1}^{n-1}\}_{\beta=1}^{n}$计算,其中$P_n$是对称群$S_n$的非平凡子群,尺寸是$|P_n|=n(n-1)$,最小距离是$d_{|P_n|}=n-1$;$C_n$是$P_n$的子群,也是一个循环群$C_n=\{c_1,\ldots,c_\beta,\ldots,c_n\}=\langle c_2\rangle$,尺寸是$|C_n|=n$,最小距离是$d_{|C_n|}=n$,$\beta=1,2,\ldots,n$;$O_n=\{o_1,\ldots,o_\alpha,\ldots,o_{n-1}\}$是$P_n$的与$C_n$不相同的另一个子群,也称为(n,n(n-1),n-1)置换群码的轨道首阵列,尺寸是$|O_n|=n-1$,最小距离是$d_{|O_n|}=n-1$,$\alpha=1,2,\ldots,n-1$,并且C_n和O_n的交集$C_n\cap O_n=e$为单位置换。在码集合P_n中,C_n将P_n划分成n-1个陪集$P_n=\{C_no_1,C_no_2,\ldots,C_no_{n-1}\}$,每一个陪集$\{C_no_\alpha\}$形成一个置换$o_\alpha$的轨道,也称为循环拉丁方(C-LS)。

[0037] 置换码集合中每一个码字由$p_{\beta\alpha}=c_\beta\circ o_\alpha$计算,它是两个置换$c_\beta$和$o_\alpha$的合成运算,不利于硬件实现,因此需要构造电路可执行的置换操作函数。由于C_n是循环阵列,可以设想用

对置换的循环移位来取代C_n的作用，从而将置换的合成运算等效地转换成循环移位操作，并能够由基本单元电路循环移位寄存器来执行，为此，首先定义下列操作函数和复合操作函数。

[0038] 构造操作函数：设T表示所有作用于置换的操作函数的集合。构造一个右移操作函数集$T_{right}=\{r_2,r_3,...,r_{n-1},r_n\}\subset T$，其任意元素$r_i\in T_{right}$是一个函数$r_i:S_n\rightarrow S_n$，并由$r_i\pi=r_i[a_1...a_i...a_n]=[a_ia_1...a_{i-1}a_{i+1}...a_n]\in S_n$来定义，称$r_i\in T_{right}$是一个置换的部分循环右移操作函数；当i＝n时，有$r_n\pi=r_n[a_1a_2...a_n]=[a_na_1a_2...a_{n-1}]\in S_n$，称$r_n$是一个置换的循环右移操作函数。类似地，构造一个左移操作函数集$T_{left}=\{l_1,l_2,...,l_{n-1}\}\subset T$，其任意元素$l_j\in T_{left}$是一个函数$l_j:S_n\rightarrow S_n$，并由$l_j\pi=l_j[a_1...a_j...a_n]=[a_1...a_{j-1}a_{j+1}...a_na_j]\in S_n$来定义，称$l_j\in T_{left}$是一个置换的部分循环左移操作函数；当j＝1时，有$l_1\pi=l_1[a_1a_2...a_n]=[a_2a_3...a_{n-1}a_na_1]\in S_n$，称$l_1$是一个置换的循环左移操作函数。

[0039] 构造循环移位的复合操作函数：根据一定的排序规则，将T_{left}或者T_{right}集合中部分或全部操作函数排列成串或者排列成不同函数幂的连乘，那么这些操作函数串或操作函数幂的积将形成复合操作函数，表示成$f_{CF}(u,\Lambda)$，其中u表示合成函数$f_{CF}(u,\Lambda)$中所包含的操作函数的数量，Λ表示操作函数的排序规则。设操作函数的排序规则Λ是：某一个函数被重复使用λ-1次，当λ＝n时，构造循环左移复合操作函数$f_{CF-l}(n-1,\Lambda)=\underbrace{l_1l_1...l_1}_{n-1}=(l_1)^{n-1}$；构造循环右移复合操作函数$f_{CF-r}(n-1,\Lambda)=\underbrace{r_nr_n...r_n}_{n-1}=(r_n)^{n-1}$。如果使这两类复合操作函数分别作用一个置换$\pi=[a_1a_2...a_n]$，那么分别得到n个置换的两个集合，表示成：$\{(l_1)^{n-1}\pi\}\overset{\Delta}{=}\{\pi,l_1\pi,l_1^2\pi,...,l_1^{n-1}\pi\}$和$\{(r_n)^{n-1}\pi\}\overset{\Delta}{=}\{\pi,r_n\pi,r_n^2\pi,...,r_n^{n-1}\pi\}$。集合$\{(l_1)^{n-1}\pi\}$和$\{(r_n)^{n-1}\pi\}$与集合$\{C_n\pi\}$一样均是置换π的轨道，即$\{C_n\pi\}=\{(l_1)^{n-1}\pi\}=\{(r_n)^{n-1}\pi\}$，这就是说三种不同的操作所形成的轨道构成等效类，但每个轨道中置换的排序均不同，因此，每个轨道中的C-LS不同。

[0040] 由此可知，陪集划分(n,n(n-1),n-1)置换群码的码集合$P_n=\{C_n0_n\}$中的循环群C_n可以用循环左移复合操作函数$(l_1)^{n-1}$或循环右移复合操作函数$(r_n)^{n-1}$取代，每个轨道$\{C_no_\alpha\}$的执行表达式为$\{C_no_\alpha\}=\{(r_n)^{n-1}o_\alpha\}=\{(l_1)^{n-1}o_\alpha\}$，枚举所有码字的表达式为α＝1,2,...,n-1，$P_n=C_n0_n=\{(r_n)^{n-1}0_n\}=\{\{(r_n)^{n-1}o_1\},\{(r_n)^{n-1}o_2\},...,\{(r_n)^{n-1}o_{n-1}\}\}=\{(l_1)^{n-1}0_n\}=\{\{(l_1)^{n-1}o_1\},\{(l_1)^{n-1}o_2\},...,\{(l_1)^{n-1}o_{n-1}\}\}$。

[0041] 下面对定理2提供的轨道首阵列0_n进行结构特征分析，然后给出0_n的某些不同的设计方法。

[0042] 轨道首阵列0_n的结构特征：一个(n,n(n-1),n-1)置换群码的轨道首阵列具有下列结构特征：其一，它是(n-1)×n的阵列，每一行都是S_n上的一个置换，并存在唯一的一列包含相同的元素a_k＝k，其中$k,a_k\in Z_n^0$或者$k,a_k\in Z_n^1$；其二，如果把相同元素的那一列去掉，余下的行和列构成一个尺寸(n-1)×(n-1)的拉丁方；其三，轨道首阵列0_n的每一行有n个不相同的相邻数对(a_μ,a_ν)，包括循环相邻数对，而轨道首阵列0_n本身包含n(n-1)个不相同的相邻(或循环相邻)数对，其中$\mu,\nu,a_\mu,a_\nu\in Z_n^0$或者$\mu,\nu,a_\mu,a_\nu\in Z_n^1$，并且$a_\mu\neq a_\nu$，μ≠ν。一般而言，当n个正整数构成数对$(a_\mu,a_\nu)$时，一共存在n(n-1)个不同数对，这成为轨道首阵列包含n

(n-1)个不相同的相邻数对的充分条件。

[0043] 轨道首阵列O_n的设计方法:满足上述三个结构特征的轨道首阵列可用显性表达式计算,如定理2,其硬件可执行的设计方案有两个。方案1,置换中包含0元素。设$a_{\alpha_1,\beta_1}\in Z_n^0$表示阵列$O_{n1}$中第$\alpha_1$行第$\beta_1$列的一个元素,其中$\alpha_1=0,1,...,n-2$表示阵列$O_{n1}$的行索引,$\beta_1=0,1,...,n-1$表示阵列$O_{n1}$的列索引,$k_1=0,1,...,n-1$表示$O_{n1}$中第$k_1$列具有相同的元素。当n是素数时,如果计算出$a_{\alpha_1,\beta_1}$是n的倍数xn时,则规定对其取模n,结果为0,即$a_{\alpha_1,\beta_1}=xn(\mathrm{mod}\,n)=0$,这里x是任意整数,轨道首阵列$O_{n1}$中每一个置换的每一个元素计算如下

[0044] $$a_{\alpha_1,\beta_1}(k_1)=[(\alpha_1+1)\times(\beta_1-k_1)+k_1](\mathrm{mod}\,n) \qquad (i)$$

[0045] $$O_{n1}(k_1)=\{o_0,o_1,...,o_{n-2}\}=\{\{a_{\alpha_1,\beta_1}(k_1)\}_{\alpha_1=0}^{n-2}\}_{\beta_1=0}^{n-1} \quad 当k_1=0,1,...,n-1时 \qquad (ii)$$

[0046] 方案2,置换中不包含0元素。设$a_{\alpha_2,\beta_2}\in Z_n^1$表示阵列$O_{n2}$中第$\alpha_2$行第$\beta_2$列的一个元素,其中$\alpha_2=1,2,...,n-1$表示阵列$O_n$的行索引,$\beta_2=1,2,...,n$表示阵列$O_{n2}$的列索引,$k_2=1,2,...,n$表示$O_{n2}$中第$k_2$列具有相同的元素。当n是素数时,如果计算出$a_{\alpha_2,\beta_2}$是n的倍数xn,则规定对其取模n,结果为n,即$a_{\alpha_2,\beta_2}=xn(\mathrm{mod}\,n)=n$,这里x是任意整数,轨道首阵列$O_{n2}$中每一个置换的每一个元素计算如下

[0047] $$a_{\alpha_2,\beta_2}(k_2)=[\alpha_2(\beta_2-k_2)+k_2](\mathrm{mod}\,n) \qquad (iii)$$

[0048] $$O_{n2}(k_2)=\{o_1,o_2,...,o_{n-1}\}=\{\{a_{\alpha_2,\beta_2}(k_2)\}_{\alpha_2=1}^{n-1}\}_{\beta_2=1}^{n} \quad 当k_2=1,2,...,n时 \qquad (iv)$$

[0049] 当$k_2=n$时,方案2的表达式(iii)和(iv)可简化为

[0050] $a_{\alpha,\beta}(n)=[\alpha\cdot\beta](\mathrm{mod}n)$ 当$\alpha=1,2,...,n-1$和$\beta=1,2,...,n$时 (v)

[0051] $$O_n=\{o_1,o_2,...,o_{n-1}\}=\{\{a_{\alpha,\beta}(n)\}_{\beta=1}^{n}\}_{\alpha=1}^{n-1}=[[\alpha\cdot\beta]_{\beta=1}^{n}]_{\alpha=1}^{n-1}(\mathrm{mod}\,n)=\{\alpha\cdot o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n) \qquad (vi)$$

[0052] 表达式(vi)与定理2的O_n计算相同。

[0053] 例2:设n=5,根据O_n的设计方案1,如果$a_{\alpha_1,\beta_1}\in Z_n^0$,那么$c_0=o_0=e=[01234]$,这时每个置换的每个元素由(i)$a_{\alpha_1,\beta_1}(k_1)=[(\alpha_1+1)\times(\beta_1-k_1)+k_1](\mathrm{mod}\,n)$计算,对不同的$k_1=0,1,2,3,4$,由(ii)的$O_{n1}(k_1)$分别计算出下列不同的轨道首阵列

[0054] $$\left\{\begin{matrix}01234,\\02413,\\03142,\\04321\end{matrix}\right\}_{k_1=0}\left\{\begin{matrix}01234,\\41302,\\31420,\\21043\end{matrix}\right\}_{k_1=1}\left\{\begin{matrix}01234,\\30241,\\14203,\\43210\end{matrix}\right\}_{k_1=2}\left\{\begin{matrix}01234,\\24130,\\42031,\\10432\end{matrix}\right\}_{k_1=3}\left\{\begin{matrix}01234,\\13024,\\20314,\\32104\end{matrix}\right\}_{k_1=4}$$

[0055] 如果用循环左移复合操作函数$(l_1)^4$或者循环右移复合操作函数$(r_5)^4$分别作用于$O_{n1}(k_1)$ ($k_1=0,1,2,3,4$)的5个轨道首阵列,所得10个置换码集合均等效。

[0056] 再设n=5,再根据O_n的设计方案2和简化方案,如果$a_{\alpha_2,\beta_2}\in Z_n^1$,那么$c_1=o_1=e=[12345]$,这时每个置换的每个元素由(iii)$a_{\alpha_2,\beta_2}(k_2)=[\alpha_2(\beta_2-k_2)+k_2]$(modn)计算或由(v)$a_{\alpha,\beta}(n)=[\alpha\cdot\beta]$(modn)计算,对不同的$k_2=1,2,3,4,5$和简化方案,由(iv)的$O_{n2}(k_2)$和(vi)的$O_n$分别计算出下列不同的轨道首阵列

[0057] $$\left\{\begin{matrix}12345,\\13524,\\14253,\\15432\end{matrix}\right\}_{k_2=1}\left\{\begin{matrix}12345,\\52413,\\42531,\\32154\end{matrix}\right\}_{k_2=2}\left\{\begin{matrix}12345,\\41352,\\25314,\\54321\end{matrix}\right\}_{k_2=3}\left\{\begin{matrix}12345,\\35241,\\53142,\\21543\end{matrix}\right\}_{k_2=4}\left\{\begin{matrix}12345,\\24135,\\31425,\\43215\end{matrix}\right\}_{k_2=5}O_5=\left\{\begin{matrix}12345,\\24135,\\31425,\\43215\end{matrix}\right\}$$

[0058] 如果用循环左移复合操作函数$(l_1)^4$或者循环右移复合操作函数$(r_5)^4$分别作用于$O_{n2}(k_2)$ $(k_2=1,2,3,4,5)$的5个轨道首阵列和简化轨道首阵列O_5，所得到的12个置换码集合均等效于由合成运算所得到的基于陪集划分的置换群码，即对k＝1,2,3,4,5，有

[0059] $$P_5=C_5O_5=\{(r_5)^4O_{52}(k_2)\}=\{(l_1)^4O_{52}(k_2)\}=\{(r_5)^4O_5\}=\{(l_1)^4O_5\}=\left\{\begin{matrix}12345, & 24135, & 31425, & 43215,\\23451, & 35241, & 42531, & 54321,\\34512, & 41352, & 53142, & 15432,\\45123, & 52413, & 14253, & 21543,\\51234, & 13524, & 25314, & 32154\end{matrix}\right\}$$

[0060] 第二部分陪集划分(n,n(n-1),n-1)置换群码的码集合产生器结构设计

[0061] 陪集划分(n,n(n-1),n-1)置换群码的码集合产生器的结构分为4个部分：包括码集合产生器体系结构、轨道首阵列产生器、ROM存储器和双向循环移位寄存器组。

[0062] 置换的二进制表示：如果用m位二进制来表示n长置换的每一个元素，那么n长的置换可以用m×n的二进制阵列来描述，m与n满足$2^{m-1}+1\leqslant n\leqslant 2^m$。

[0063] 码集合产生器体系结构：由轨道首阵列产生器、ROM存储器和双向循环移位寄存器组三个部分组成，如图1所示。轨道首阵列产生器的原理电路是以表达式(i)-(vi)为依据，构造生成轨道首阵列的原理电路，具体工作过程是执行表达式(vi)的计算$\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$，产生包含n-1个置换的轨道首阵列$O_n=\{o_1,o_2,\ldots,o_{n-1}\}$。ROM存储器的作用是首先存储轨道首阵列产生器的输出结果$O_n=\{o_1,o_2,\ldots,o_{n-1}\}$，然后存储双向循环移位寄存器组的输出结果$P_n=\{\{(l_1)^{n-1}o_1\},\{(l_1)^{n-1}o_2\},\ldots,\{(l_1)^{n-1}o_{n-1}\}\}$或者$P_n=\{\{(r_n)^{n-1}o_1\},\{(r_n)^{n-1}o_2\},\ldots,\{(r_n)^{n-1}o_{n-1}\}\}$。双向循环移位寄存器组的作用是对一个置换执行循环左移复合操作函数$(l_1)^{n-1}$或者循环右移复合操作函数$(r_n)^{n-1}$的操作，具体是对轨道首置换o_α进行n-1次循环左移或者n-1次循环右移操作，实现每个轨道首置换o_α的轨道$\{(l_1)^{n-1}o_\alpha\}$或者$\{(r_n)^{n-1}o_\alpha\}$，α＝1,2,...,n-1；由于每个轨道$\{(l_1)^{n-1}o_\alpha\}$或者$\{(r_n)^{n-1}o_\alpha\}$包含n个置换，如果对每个轨道的生成过程重复n-1次，则形成陪集划分(n,n(n-1),n-1)置换群码的码集合，具体计算表达式为$P_n=C_nO_n=\{(l_1)^{n-1}O_n\}=\{\{(l_1)^{n-1}o_1\},\{(l_1)^{n-1}o_2\},\ldots,\{(l_1)^{n-1}o_{n-1}\}\}$或者$P_n=C_nO_n=\{(r_n)^{n-1}O_n\}=\{\{(r_n)^{n-1}o_1\},\{(r_n)^{n-1}o_2\},\ldots,\{(r_n)^{n-1}o_{n-1}\}\}$。

[0064] 轨道首阵列产生器：见附图2。在对电路结构进行优化的情况下，结构参数设计如下：n为任意素数，为了避免衰落干扰使幅值衰减到0与码字中码元为0的情况发生冲突，取$a_{\alpha,\beta}\in Z_n^1$保证每个置换码字中不出现0元。为了便于码元跟踪，取k_2＝n表示轨道首阵列的最后一列是相同列，其值为n，这样可以使表达式(i)和(iii)最大程度的简化为表达式(v)：$a_{\alpha,\beta}(n)=[\alpha\cdot\beta]\,(\mathrm{mod}n)$，使轨道首阵列$O_n$的计算简化为

$O_n=\{o_1,o_2,\ldots,o_{n-1}\}=\{\alpha o_1\}_{\alpha=1}^{n-1}\,(\mathrm{mod}\,n)$，其中α＝1,2,...,n-1表示轨道首阵列包含n-1个置换，β＝1,2,...,n表示每个置换包含n个元素。

[0065] 轨道首阵列产生器的功能是当初始置换是o_1=e=[12...n]时，执行n-1个轨道首置换$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)=\{o_1,2o_1,...,(n-1)o_1\}(\mathrm{mod}\,n)$的计算，产生n-1个轨道首置换，每产生一个置换，就通过总线传给ROM存储器。

[0066] 轨道首阵列产生器由五部分构成：n个并行运行输入缓存器(10)、n个并行运行正整数加法器(11)、n个并行运行modn计算器(12)、n个并行运行输出缓存器(13)、n输入单输出开关(14)和使能信号产生器(15)。各部分的工作原理描述如下：

[0067] n个并行运行输入缓存器(10)由n个m位的寄存器构成，每个寄存器以m位二进制存储n个输入数据中的一个，每一个缓存器有m根并行的数据线输入和输出。输入初始置换o_1=e=[12...n]到n个并行运行输入缓存器(10)中，轨道首阵列产生器开始工作。

[0068] n个并行运行正整数加法器(11)用于将$O_n=\{\alpha o_1\}_{\alpha=1}^{n-1}=\{o_1,2o_1,...,(n-1)o_1\}$中的乘法运算{$o_1$,2$o_1$,...,(n-1)$o_1$}转换成对初始置换$o_1$=[12...n]中每个元素的累加运算，主要完成$\{\alpha o_1\}_{\alpha=1}^{n-1}$计算；初始单位置换不需要累加，直接传输到输出缓存器，因此，需要做n-2次累加，才能完成集合$\{\alpha o_1\}_{\alpha=1}^{n-1}$的运算；n个并行运行正整数加法器(11)的每一个加法器由m'个二进制全加器和m'位B寄存器构成，其中$m<m'\le\lceil\log_2(n-1)^2\rceil$，m根数据线并行输入，m'根数据线并行输出；每个二进制全加器的一个输入端接收输入缓存器的数据，另一个输入端与B寄存器的输出端相连，二进制全加器的输出端与B寄存器的输入端相连；n个并行运行正整数加法器(11)的工作原理是：在使能信号E=1时，每个加法器将上一次的求和结果，即B寄存器中的内容与n个并行运行输入缓存器(10)的输入结果相加一次，将求和结果保存在B寄存器中，并将B寄存器中的内容输出给n个并行运行modn计算器(12)；当使能信号E=0时，加法器不工作。

[0069] n个并行运行modn计算器(12)用于完成$\{\alpha o_1\}_{\alpha=1}^{n-1}(\mathrm{mod}\,n)$计算，具体是对n个并行运行正整数加法器(11)中B寄存器传来的数据进行modn计算；每一个modn计算器由一个两输入端单输出端通用modn计算器、m位C寄存器和m位D寄存器构成，m'根数据线并行输入，m根数据线并行输出；通用modn计算器的一个输入端有m'位并行输入数据线连接B寄存器的输出端，另一个输入端有m位并行输入数据线连接C寄存器的输出端，其一个输出端有m位并行输出数据线；C寄存器存储不变数据n，D寄存器用于存储通用modn计算器的输出结果；如果D寄存器的数据|x|不为0，则输出D寄存器的数据，如果D寄存器数据|x|为0，则输出C寄存器的数据。

[0070] n个并行运行输出缓存器(13)与n个并行运行输入缓存器(10)的结构相同，即由n个m位的寄存器构成，其作用是存储当前生成的轨道首置换；当n个并行运行输出缓存器(13)的第n-1个缓存器的当前数据准备好时，向n输入单输出开关(14)的第一个开关发送信号，使其闭合。

[0071] n输入单输出开关(14)用于将n个并行运行输出缓存器(13)的n个数据的每一个串行输出到总线上，从1到n每接通一个开关，相当于每一个输出缓存器的m根数据线与m根并行总线接通；当n个并行运行输出缓存器(13)的第n-1个缓存器准备好当前数据时，向n输入单输出开关(14)第一个开关，发出闭合开关的信号；当第n个开关闭合，将最后一位数据通过总线传输到ROM中时，输出一个高电平信号至使能信号产生器(15)的输入端。

[0072] 使能信号产生器(15)为n个并行运行正整数加法器(11)提供使能信号，它由二进制加1计数器和单稳态触发器构成，一根输入信号线，一根输出信号线，常态输出低电平；使能信号产生器的输入端与n输入单输出开关(14)的第n个开关的输出控制信号线相连，输出端与n个并行运行正整数加法器(11)的使能端E相连；使能信号产生器(15)的工作原理是：当n输入单输出开关(14)的第n个开关闭合时，使能信号产生器(15)工作，二进制加1计数器做一次加1操作，并使单稳态触发器产生持续时间为1个cp的高电平脉冲，输出到n个并行运行正整数加法器(11)的使能端，使E＝1；当n输入单输出开关(14)的第n个开关断开时，使能信号产生器(15)不工作，并保持E＝0不变。二进制加1计数器加n-1次时，使能信号产生器(15)输出低电平。

[0073] ROM存储器：见附图3。ROM存储器(16)可以是可编程存储器PROM，可擦除可编程存储器EPROM、电可擦除可编程存储器E^2PROM或闪存(flash memory)。ROM存储器(16)的存储结构是：一个置换的每一个元素用m位二进制表示，如一个置换的第一个元素用m位二进制$b_{1,1},b_{2,1},\ldots,b_{m-1,1},b_{m,1}$表示，最后一个元素用m位二进制$b_{1,n},b_{2,n},\ldots,b_{m-1,n},b_{m,n}$表示，其中$b_{i,j}$(i＝0,1,...,m-1,j＝0,1,...,n-1)是取值0或1的二进制数值。每个置换的一个元素的m位二进制占用m个存储单元，定义为存储器的一个元素存储字；一个置换占用n个元素存储字，n-1个轨道首置换占用n(n-1)个元素存储字，n(n-1)个置换码字占用$n^2(n-1)$个元素存储字。ROM存储器(16)有m位并行数据输入端和m位并行数据输出端。ROM存储器(16)的具体工作过程为：当Wr＝1时，一个元素存储字的m位数据并行输入；当Rd＝1时，一个元素存储字的m位数据并行输出。当Wr＝0和Rd＝0时，ROM存储器(16)不工作。

[0074] 双向循环移位寄存器组：见附图4。双向循环移位寄存器组(17)用于实现循环左移复合操作函数$(l_1)^{n-1}$或循环右移复合操作函数$(r_n)^{n-1}$对一个置换的操作，执行轨道$\{(l_1)^{n-1}o_\alpha\}$与$\{(r_n)^{n-1}o_\alpha\}$的生成计算实现，以及码集合$\{(l_1)^{n-1}0_n\}$与$\{(r_n)^{n-1}0_n\}$的生成计算。其存储结构为：n维置换矢量的每一个元素可以用m维的二进制序列来表示，每一个n维置换矢量映射成m×n维的二进制数阵列，对应m×n个触发器构成m行n列的触发器阵列，m行的每一行由n个触发器形成既能循环左移又能循环右移的寄存器，即n个触发器构成双向循环移位寄存器，共需要m个这样的双向循环移位寄存器构成m个双向循环移位寄存器组，其中第一个循环移位寄存器存储n位二进制数$b_{1,1},b_{1,2},\ldots,b_{1,n-1},b_{1,n}$，第m个循环移位寄存器存储n位二进制数$b_{m,1},b_{m,2},\ldots,b_{m,n-1},b_{m,n}$(注意该阵列是m×n，ROM存储器(16)的阵列是n×m)。在循环左移回路中串接m个并行开关(18)，开关闭合，则执行m个数据并行的循环左移操作，开关断开，则执行m个数据并行的左移输入和左移输出操作。设置两个控制信号输入端REG-in和REG-out，可以组合四种控制信号00,01,10,11，分别对应双向循环移位寄存器组的四种工作状态：左移输入，左移输出，循环左移和循环右移。双向循环移位寄存器组(17)的工作过程描述如下：

[0075] 过程a——执行一个置换的输入。当REG-in＝0、REG-out＝0和Rd＝1时，循环左移回路的m个并行开关(18)断开，将ROM存储器(16)中的第一个轨道首置换转移到双向循环移位寄存器组(17)中，此期间循环移位寄存器组执行m位并行n位串行左移输入操作；

[0076] 过程b——用循环左移产生一个新置换。当REG-in＝0和REG-out＝1时，循环左移回路的m个并行开关(18)闭合，双向循环移位寄存器组(17)执行m位并行n位串行循环左移操作，产生一个新的置换；

[0077] 过程c——执行一个置换的输出。当REG-in＝1、REG-out＝0和Wr＝1，循环左移回路的m个并行开关(18)闭合，双向循环移位寄存器组(17)完成两个操作：通过m位并行n位串行左移输出操作，将过程b所产生的当前置换转移到ROM存储器(16)中，同时完成当前置换的m位并行n位串行循环左移操作，使过程b所产生的置换得以保留；

[0078] 过程d——产生一个$\{(l_1)^{n-1}o_\alpha\}$轨道。由过程b和过程c组合而成，在此期间循环左移回路的m个并行开关(18)闭合，这两个过程轮流工作：即在1个cp时钟脉冲期间，REG-in＝0和REG-out＝1，双向循环移位寄存器组(17)执行一次m位并行n位串行循环左移操作，得到一个新置换；在接着的n个cp时钟脉冲期间，REG-in＝1、REG-out＝0和Wr＝1，双向循环移位寄存器组(17)同时执行对当前置换的m位并行n位串行左移输出操作和m位并行n位串行循环左移操作，保存当前置换，并将其转移到ROM存储器(16)中。过程d相当于对一个轨道首置换o_α完成$(l_1)^{n-1}$操作，产生一个完整的$\{(l_1)^{n-1}o_\alpha\}$轨道，并将由轨道$\{(l_1)^{n-1}o_\alpha\}$所产生的n-1个置换保存到ROM存储器(16)中。

[0079] 过程e——产生码集合$\{(l_1)^{n-1}0_n\}$。由过程a和过程d组合而成，对过程e执行n-1次重复操作，完成一个陪集划分(n,n(n-1),n-1)置换群码的码集合$\{(l_1)^{n-1}0_n\}$的产生过程。

[0080] 过程b'——用循环右移产生一个新置换。将过程b修改为过程b'：当REG-in＝1和REG-out＝1时，循环左移回路的m个并行开关断开，双向循环移位寄存器组(17)执行m位并行n位串行循环右移操作，产生一个新的置换。

[0081] 过程d'：产生一个$\{(r_n)^{n-1}o_\alpha\}$轨道。由过程b'和过程c组合而成，等效于完成置换o_α的轨道$\{(r_n)^{n-1}o_\alpha\}$的生成，并在ROM存储器(16)中存储$\{(r_n)^{n-1}o_\alpha\}$。

[0082] 过程e'：产生码集合$\{(r_n)^{n-1}0_n\}$。由过程a和过程d'组合而成，对过程e'执行n-1次重复操作，完成一个陪集划分(n,n(n-1),n-1)置换群码的码集合$\{(r_n)^{n-1}0_n\}$的产生过程。

[0083] 本领域的技术人员容易理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

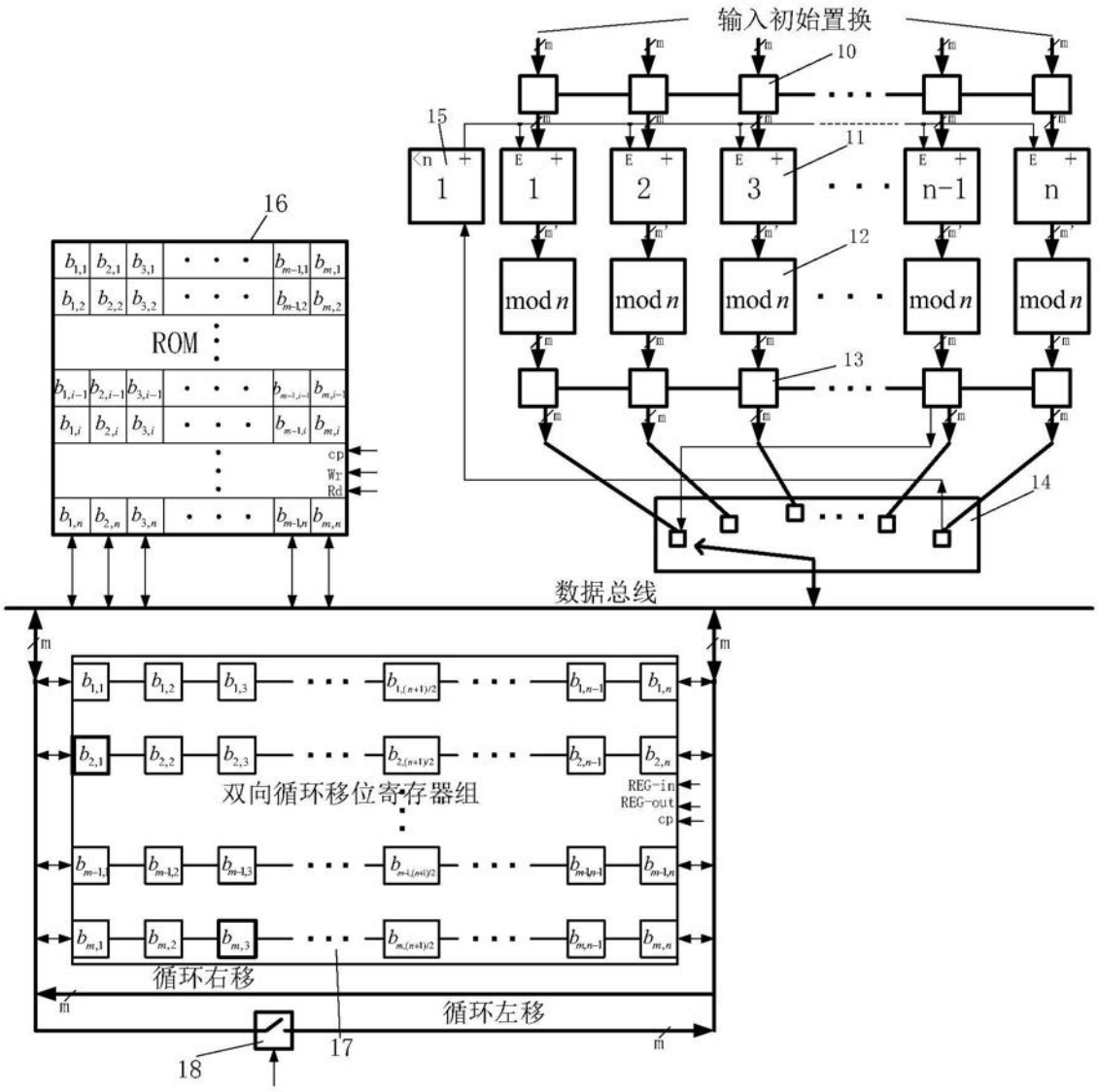

输入初始置换
10
15
11
16
12
13
14
ROM
cp
Wr
Rd
mod n
数据总线
双向循环移位寄存器组
REG-in
REG-out
cp
循环右移
循环左移
17
18

图1

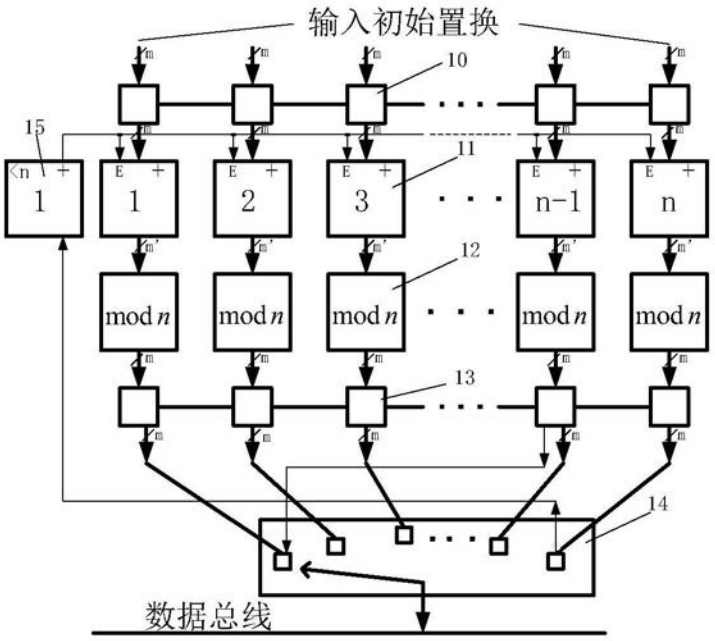


图2

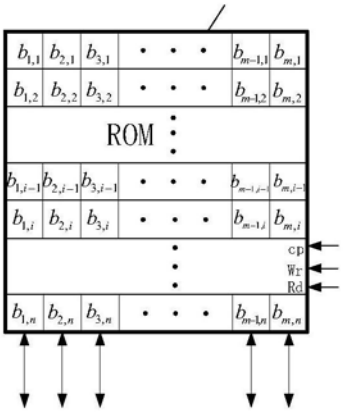


图3

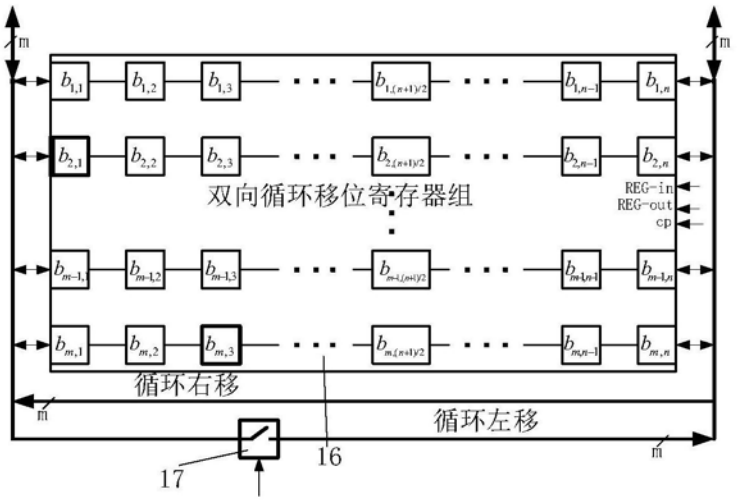


图4