Information Sciences 222 (2013) 784–794

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A generalization of the Hall's sextic residue sequences

Xiaoni Du [a], Zhixiong Chen [b,*]

[a] College of Math. and Inform. Sci., Northwest Normal University, Lanzhou, Gansu 730070, PR China
[b] Department of Mathematics, Putian University, Putian, Fujian 351100, PR China

ARTICLE INFO

Article history:
Received 6 January 2009
Received in revised form 22 March 2012
Accepted 25 July 2012
Available online 15 August 2012

Keywords:
Stream cipher
Pseudorandom sequence
Generalized cyclotomic sequence
Hall's sequence
Linear complexity
Trace function representation

ABSTRACT

Let p be a prime with $6|(p-1)$ and integer $m \geqslant 1$. As a generalization of the Hall's sextic residue sequences, we introduce some families of generalized cyclotomic binary sequences over the residue class ring modulo p^m by defining sextic generalized cyclotomic residue classes. We determine the values of the linear complexity, which are large enough to resist security attacks using the Berlekamp–Massey algorithm. We also investigate the trace function representation for the resulting sequences when $m = 2$.

1. Introduction

Let p be an odd prime and integer $m \geqslant 1$. We identify $\mathbb{Z}_{p^m}$, the residue ring modulo p^m, with the set $\{0, 1, \ldots, p^m - 1\}$. We also denote by $\mathbb{Z}^*_{p^m}$ the set of unit elements of $\mathbb{Z}_{p^m}$. Since $\mathbb{Z}^*_{p^m}$ is a cyclic group under the multiplicative operation, let g be one of its generators (or primitive elements). Then we have

$$\mathbb{Z}^*_{p^m} = \{g^i : i = 0, 1, \ldots, \varphi(p^m)\},$$

where $\varphi(-)$ is the Euler totient function. By defining different partitions of $\mathbb{Z}^*_{p^m}$, the ring $\mathbb{Z}_{p^m}$ is extensively applied to constructing pseudorandom sequences in the literature. A typical partition is the (generalized) cyclotomic classes, see below for the definition.

In this paper, we always suppose that g is a primitive element modulo p^2. We note that in this case g is a primitive element modulo p^n for any $n \geqslant 1$ [16]. That is, the order of g in $\mathbb{Z}^*_{p^n}$ is $\mathrm{ord}_{p^n}(g) = \varphi(p^n) = p^{n-1}(p-1)$. Let d be an *even* integer satisfying $d|(p-1)$. Now for each n, we get the *(generalized) cyclotomic classes* of $\mathbb{Z}^*_{p^n}$ by defining

$$D_0^{(n)} = (g^d) = \left\{g^{dk}(\mathrm{mod} p^n) : \ k = 0, 1, \ldots, \frac{\varphi(p^n)}{d} - 1\right\},$$

$$D_l^{(n)} = g^l D_0^{(n)} = \left\{g^l x(\mathrm{mod} p^n) : \ x \in D_0^{(n)}\right\}, \quad l = 1, \ldots, d-1,$$

which give a partition of $\mathbb{Z}^*_{p^n}$. Let

[*] Corresponding author.
E-mail addresses: ymLdxn@126.com (X. Du), ptczx@126.com (Z. Chen).

0020-0255/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2012.07.048

$$R^{(n)} = p\mathbb{Z}_{p^{n-1}} = \{0, p, 2p, \ldots, (p^{n-1}-1)p\},$$

we have

$$\mathbb{Z}_{p^n} = \mathbb{Z}^*_{p^n} \cup R^{(n)} = \left(D_0^{(n)} \cup D_1^{(n)} \cup \cdots \cup D_{d-1}^{(n)}\right) \cup R^{(n)}.$$

Thus we represent the ring $\mathbb{Z}_{p^m}$ as follows

$$\begin{aligned}
\mathbb{Z}_{p^m} &= D_0^{(m)} \cup D_1^{(m)} \cup \cdots \cup D_{d-1}^{(m)} \cup p\mathbb{Z}_{p^{m-1}} \\
&= \left(D_0^{(m)} \cup pD_0^{(m-1)}\right) \cup \cdots \cup \left(D_{d-1}^{(m)} \cup pD_{d-1}^{(m-1)}\right) \cup p^2\mathbb{Z}_{p^{m-2}} \\
&\cdots \\
&= \left(\bigcup_{n=1}^{m} p^{m-n} D_0^{(n)}\right) \bigcup \cdots \bigcup \left(\bigcup_{n=1}^{m} p^{m-n} D_{d-1}^{(n)}\right) \bigcup \{0\}.
\end{aligned}$$

Assume that

$$C_l = \bigcup_{n=1}^{m} p^{m-n} D_l^{(n)}, \quad l = 0, 1 \ldots, d-1, \tag{1}$$

then we have

$$\mathbb{Z}_{p^m} = \bigcup_{i=0}^{d-1} C_i \cup \{0\} \quad \text{and} \quad C_i \cap C_j = \emptyset, \quad i \neq j, \quad i, \quad j = 0, \ldots, d-1,$$

where $\emptyset$ denotes the empty set.

So one can construct a p^m-periodic binary sequence $\{s_t\}_{t \geqslant 0}$ by defining

$$s_t = \begin{cases} 1, & \text{if } t (\text{mod } p^m) \in C_0 \cup \cdots \cup C_{\frac{d}{2}-1}, \\ 0, & \text{otherwise}, \end{cases} \quad t \geqslant 0, \tag{2}$$

where $C_0 \cup \cdots \cup C_{\frac{d}{2}-1}$ is called the *characteristic set* of $\{s_t\}_{t \geqslant 0}$. We note that $\{s_t\}_{t \geqslant 0}$ is called a *cyclotomic sequence* for $m = 1$ or a *generalized cyclotomic sequence* for $m \geqslant 2$. Some special cases have been investigated in the literature, see Table 1, in which the symbol "$\surd$" means that the trace function representation of the corresponding sequences has been investigated.

In this paper, we will consider $\{s_t\}_{t \geqslant 0}$ defined in (2) and its related sequences when $m \geqslant 1$ and $d = 6$.

Definition 1. Let distinct integers $u, v, w \in \mathbb{Z}_6 = \{0, 1, \ldots, 5\}$, which is the residue class ring modulo 6. The triple subset $\{u,v,w\}$ is admissible over $\mathbb{Z}_6$ if there exists an $\ell \in \mathbb{Z}_6$ such that

$$\{u + \ell(\text{mod}6), v + \ell(\text{mod}6), w + \ell(\text{mod}6)\} = \mathbb{Z}_6 \setminus \{u, v, w\}.$$

One can easily verify that all admissible triples over $\mathbb{Z}_6$ are

$$\{0,1,2\};\ \{1,2,3\};\ \{2,3,4\};\ \{3,4,5\};\ \{4,5,0\};\ \{5,0,1\};\ \{1,3,5\};\ \{0,2,4\}.$$

Proposition 1. *Each admissible triple $\{u, v, w\}$ over $\mathbb{Z}_6$ satisfies*

$$\{u, v, w, u+3(\text{mod } 6), v+3(\text{mod } 6), w+3(\text{mod } 6)\} = \mathbb{Z}_6.$$

Proof. Clearly. □

Now we introduce the new sequences. Let $\mathcal{A}$ be the set of all admissible triples over $\mathbb{Z}_6$.

Table 1
Some known cyclotomic sequences and generalized cyclotomic sequences.

m, d	Characteristic set	Linear complexity	Trace	Refs.
$m = 1$, $d = 2$	C_1	$\left\{\frac{p\pm1}{2}, p-1, p\right\}$	$\surd$	[6,13,14]
$m = 1$, $d = 6$	$C_0 \cup C_1 \cup C_2$	$\left\{\frac{p+1}{2}, p\right\}$	$\surd$	[8]
$m = 1$, $d = 6$	$C_0 \cup C_1 \cup C_3$	$\left\{\frac{p-1}{6}, p\right\}$	$\surd$	[9,10]
$m = 2$, $d = 2$	$C_1 \cup \{0\}$	$\left\{\frac{p^2+1}{2}, p^2\right\}$	–	[19,1,17]
$m = 3$, $d = 2$	$C_1 \cup \{0\}$	$\left\{\frac{p^3\pm1}{2}, p^3-1, p^3\right\}$	–	[11]
$m \geqslant 2$, $d = 2$	$C_1 \cup \{0\}$	$\left\{\frac{p^m\pm1}{2}, p^m-1, p^m\right\}$	–	[18,12]