Des. Codes Cryptogr. (2016) 78:679–691
DOI 10.1007/s10623-014-0024-8

Partially user-irrepressible sequence sets and conflict-avoiding codes

Yuan-Hsun Lo · Wing Shing Wong · Hung-Lin Fu

Received: 3 December 2013 / Revised: 13 June 2014 / Accepted: 10 November 2014 /
Published online: 22 November 2014

Abstract In this paper we give a partial shift version of user-irrepressible sequence sets and conflict-avoiding codes. By means of disjoint difference sets, we obtain an infinite number of such user-irrepressible sequence sets whose lengths are shorter than known results in general. Subsequently, the newly defined partially conflict-avoiding codes are discussed.

Keywords User-irrepressible protocol sequence · Conflict-avoiding code · Disjoint difference set

Mathematics Subject Classification 94B25 · 94C15 · 05B10

1 Introduction

Protocol sequences, which were first introduced in [15], provide feedback-free solutions for media access control (MAC) in communication networks. While the dominant MAC standards for cell-based systems, including cellular networks and Wireless LAN's, are feedback-based, the feedback-free approach has a strong appeal to networks without a backbone hier-

Communicated by J. D. Key.

Y.-H. Lo (✉)
Department of Mathematics, National Taiwan Normal University, Taipei 116, Taiwan
e-mail: yhlo0830@gmail.com

W. S. Wong
Department of Information Engineering, The Chinese University of Hong Kong, Shatin, New Town, Hong Kong
e-mail: wswong@ie.cuhk.edu.hk

H.-L. Fu
Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan
e-mail: hlfu@math.nctu.edu.tw

archy. For example, recent works have begun to explore the application of protocol sequences to ad hoc networks, such as *vehicular ad hoc network* (VANET) [25,26].

A fundamental challenge in MAC design is due to the lack of synchronicity among different users who try to access the shared medium. Protocol sequences are constructed specifically to handle the asynchronous reality. Intuitively, a good design should ensure that no matter how the sequences are shifted with respect to one another, each sequence should permit its affiliated user to transmit at least one packet without suffering interference from other users. Protocol sequence sets with this property are commonly referred to as possessing the user-irrepressible (UI) property [21,24]. It turns out that an important approach to construct UI protocol sequence sets is by means of CAC, which stands for Conflict-avoiding Codes [12,16,20]. Therefore, there is a close tie between protocol sequences and CAC. The objective of finding UI protocol sequence sets with large number of sequence elements with short sequence period can be transformed to finding CAC sets with large code size and short code length.

Although it is difficult to ensure precise user-synchronicity in multi-user communication systems, in many applications it is relatively easy to maintain some rough degree of user synchronicity. For example, mobile users may have access to a global clock via the GPS, which provides rough time synchronization. However, due to propagation delays and other engineering restrictions, transmitted signals cannot be completely synchronized (see for example [25]). For partially synchronous applications, protocol sequence sets are only required to observe the UI property for relative shifts up to a certain magnitude.

In this paper, we define a partial shift version of user-irrepressible sequence sets in Sect. 2. Two prior known constructions: TDMA and code-based scheduling (via Galois field or Reed-Solomon code), are then introduced to provide some quick baseline comparison. Next, we introduce a new concept, called partially conflict-avoiding code (PCAC), in order to build a partially user-irrepressible sequence set. The definition of a partially conflict-avoiding code will be given in Sect. 3 together with its graphic representation. A useful tool in combinatorial design called disjoint difference set is also introduced. In Sect. 4 we provide a few families of partially user-irrepressible sequence sets by means of disjoint difference sets. Comparison of the PCAC approach with TDMA and code-based scheduling will also be given in Sect. 4. Finally, we study the optimal partially conflict-avoiding codes of small weights in Sect. 5.

2 User-irrepressible sequences

Let n be a positive integer and X be a binary sequence of length n. The *cyclic shift operator*, $\mathcal{R}$, on X is defined by

$$\mathcal{R}(X(0), X(1), \ldots, X(n-1)) := (X(n-1), X(0), \ldots, X(n-2)),$$

where $X(i)$ denotes the i-th component of X. The following definition is an extension of *user-irrepressible* property which is proposed in [20].

Definition 1 Let n, k, Δ be integers satisfying $0 < k \leq n$ and $0 \leq \Delta < n$. Consider a sequence set with N ($\geq k$) elements, each having a length n. Each element is represented by a shifted version that is obtained by applying the operator $\mathcal{R}$ for an arbitrary number (say τ) of times, where $0 \leq \tau \leq \Delta$. Denote by $\mathbf{M}$ the $k \times n$ matrix obtained by stacking any k representations one above the other. The sequence set is $(n, k; \Delta)$-*User-Irrepressible* (UI for short) if we can always find a $k \times k$ submatrix of $\mathbf{M}$ which is a permutation matrix.

An $(n, k; \Delta)$-UI sequence set is obviously a solution to the problem we formulated in Sect. 1. Throughout this paper, we use N, k, and n to denote respectively the number of potential users in a system, the maximum number of active users at any time, and the common sequence period.

It is not hard to find an $(n, k; \Delta)$-UI sequence set. One simple way is based on the TDMA approach. For $0 \le i \le k-1$, let X_i be the binary sequence of length $k(\Delta+1)$ composed of all zeroes except for the $i(\Delta+1)$-th position, that is, $X_i(i(\Delta+1)) = 1$. Then $\{X_0, X_1, \ldots, X_{k-1}\}$ is obviously an $(n, k; \Delta)$-UI sequence set of length $n = k(\Delta+1)$ and size $N = k$. In practice, however, the set size N is in theory larger than k. An alternative construction for the case where N is much larger than k is based on Galois fields. After appending Δ 'zeroes' to all entries of each sequence constructed in [9], we have the following result.

Theorem 1 ([9,25]) *Given a prime power q and a positive integer m. Then for any $\Delta \ge 0$, there exists a $((\Delta+1)q^2, k; \Delta)$-UI sequence set of size $N = q^m$, where the positive integer k satisfies*

$$q \ge (k-1)(m-1) + 1. \tag{1}$$

In general, it provides an $(n, k; \Delta)$-UI sequence set of size N with length

$$n = O\left(\Delta k^2 m^2\right) = O\left(\frac{\Delta k^2 \ln^2 N}{\ln^2 k}\right).$$

Note that the parameter m above must be larger than 1 to make (1) meaningful. It is worth mentioning that in [18], a solution based on Reed-Solomon Codes was proposed which has the same order behavior.

3 Combinatorial structure

In this section, we define the new concept of partially conflict-avoiding codes and introduce two relevant combinatorial structures for analyzing them: graph packings and disjoint difference sets. The connection of these terms with UI sequence sets will be shown as

$$\begin{array}{ccc} (n, k; \Delta)\text{-UI sequence set} & \underset{\text{Prop. 1}}{\Longleftarrow} & \text{PCAC}_\Delta(n, k) \\ & & \Updownarrow \text{ Prop. 2} \\ (n, k, r)\text{-DDS} & \underset{\text{Prop. 3}}{\Longrightarrow} & (k, \Delta)\text{-packing of } K_n \end{array} \tag{2}$$

3.1 CAC and PCAC$_\Delta$

Given a binary sequence X, the *weight* of X, denoted by $\omega(X)$, is the number of 'ones' in it. For integers $n > k > 0$, let $\mathcal{S}(n, k)$ denote the set of all binary sequences of length n and weight k. The *Hamming cross-correlation* of binary sequences X and Y is defined by

$$H(X, Y) := \max_{\tau} \sum_{i=0}^{n-1} X(i)\mathcal{R}^\tau Y(i), \tag{3}$$

where τ goes from 0 up to $n-1$. Note that $H(X, X) = \omega(X)$ for all X and $H(X, Y) \ge 1$ if $X \ne Y$.

Definition 2 A set $\mathcal{C} \subseteq \mathcal{S}(n, k)$ is a *conflict-avoiding code*, CAC, of length n and weight k if $H(X, Y) = 1$ for any distinct $X, Y \in \mathcal{C}$.

Denote by $\mathrm{CAC}(n,k)$ the class of all CACs of length n and weight k. The maximum size of codes in $\mathrm{CAC}(n,k)$ is denoted by $M(n,k)$. A code $\mathcal{C} \in \mathrm{CAC}(n,k)$ is said to be *optimal* if $|\mathcal{C}| = M(n,k)$. For more results on optimal CACs, please refer to [11,12,14,16,20].

In what follows, we generalize the constraint that τ is arbitrary in (3). Assume that Δ, an integer between 0 and $n-1$, is the maximum number of relative cyclic shifts. Then the *Hamming cross-correlation of* $X, Y \in \mathcal{S}(n,k)$ *with respect to* Δ is defined by

$$H_\Delta(X,Y) := \max_{0\le\tau\le\Delta} \sum_{i=0}^{n-1} X(i)\mathcal{R}^\tau Y(i). \tag{4}$$

Definition 3 Let n, k, Δ be integers with $0 < k < n$ and $0 \le \Delta < n$. A set $\mathcal{C} \subseteq \mathcal{S}(n,k)$ is a *partially conflict-avoiding code with respect to* Δ, PCAC_Δ, of length n and weight k if $H_\Delta(X,Y) \le 1$ for any distinct $X, Y \in \mathcal{C}$.

Similarly, $\mathrm{PCAC}_\Delta(n,k)$ denotes the class of all PCAC_Δs of length n and weight k, and $M_\Delta(n,k)$ denotes the maximum size of codes in $\mathrm{PCAC}_\Delta(n,k)$. It is obvious that a PCAC_Δ admits the UI-property.

Proposition 1 *A code* $\mathcal{C} \in PCAC_\Delta(n,k)$ *is an* $(n,k;\Delta)$*-UI sequence set with size* $N = |\mathcal{C}|$.

Let n, k, Δ be integers satisfying the setting of Definition 3. It is clear that

$$\mathrm{PCAC}_\Delta(n,k) \supseteq \mathrm{PCAC}_{\Delta+1}(n,k) \supseteq \cdots \supseteq \mathrm{PCAC}_{n-1}(n,k) = \mathrm{CAC}(n,k),$$

and thus

$$M_\Delta(n,k) \ge M_{\Delta+1}(n,k) \ge \cdots \ge M_{n-1}(n,k) = M(n,k).$$

Here is an interesting observation.

Lemma 1 *Let* n, k *be integers with* $n > k > 0$. *If* Δ *is an integer with* $\lfloor \frac{n}{2} \rfloor \le \Delta < n$, *then* $M_\Delta(n,k) = M(n,k)$.

Proof We first claim that $H_\Delta(X,Y) \ge 1$ for any two distinct sequences X, Y in $\mathcal{S}(n,k)$. Assume to the contrary that $H_\Delta(X,Y) = 0$. Pick any two indices i, j with $X(i) = Y(j) = 1$. For every $\tau = 0, 1, \ldots, \Delta$, since $X(i)\mathcal{R}^\tau Y(i) = 0$, we have $Y(i-\tau) = 0$, where the addition is taking modulo n. Similarly, there are consecutive $\Delta+1$ 'zeroes' from $X(j-\Delta)$ to $X(j)$. Since $X(i) = Y(j) = 1$, those $2(\Delta+1)$ indices are distinct (see Fig. 1). Then we have $2(\Delta+1) \le n$, which contradicts to $\lfloor \frac{n}{2} \rfloor \le \Delta$.

Let $\mathcal{C} \in \mathrm{PCAC}_\Delta(n,k)$. Above argument promises that $H_\Delta(X,Y) = 1$ for any two distinct sequences $X, Y \in \mathcal{C}$. We now claim that $\mathcal{C} \in \mathrm{CAC}(n,k)$. Assume to the contrary that there exist two distinct sequences $X, Y \in \mathcal{C}$ so that $H(X,Y) \ge 2$. By symmetry there exist indices i_1, i_2, j_1, j_2 such that $X(i_1) = X(i_2) = 1$ and $Y(j_1) = Y(j_2) = 1$, where $i_1 + \tau \equiv j_1 \pmod n$ and $i_2 + \tau \equiv j_2 \pmod n$ for some $\tau \le \Delta$. This contradicts to $H_\Delta(X,Y) = 1$. Hence the proof is completed. □

3.2 Graphic representation

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ denote the ring of residues modulo n. Let K_n denote the complete graph of order n whose vertices are labeled by elements in $\mathbb{Z}_n$. Given any subset $A \subseteq \mathbb{Z}_n$, let C_A denote the *clique* induced by A, namely, the subgraph with vertex set A whose vertices

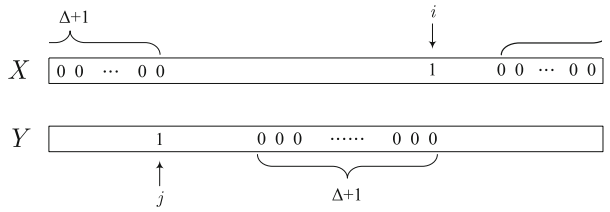

Fig. 1 Illustration of $X(i) = Y(j) = 1$

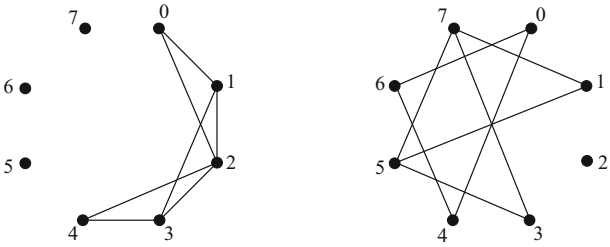

Fig. 2 $G_2(\{0, 1, 2\})$ and $G_2(\{3, 5, 7\})$ in K_8

are pairwise adjacent. A clique of order t is usually called a t-clique. Given an integer Δ with $0 \le \Delta < n$, the *supporting graph* of A with respect to Δ is defined as

$$G_\Delta(A) := C_A \cup C_{A+1} \cup \cdots \cup C_{A+\Delta},$$

where $A + \tau = \{i + \tau \pmod n : i \in A\}$. By putting the n vertices of K_n in clockwise direction from 0 to $n-1$, $G_\Delta(A)$ can be viewed as the union of $(\Delta + 1)$ $|A|$-cliques, each of which is obtained by rotating C_A clockwise step by step. For example, let $n = 8$, $\Delta = 2$ and $A = \{0, 1, 2\}$, $B = \{3, 5, 7\}$, then $A + 1 = \{1, 2, 3\}$, $A + 2 = \{2, 3, 4\}$, $B + 1 = \{4, 6, 0\}$ and $B + 2 = \{5, 7, 1\}$. See Fig. 2 for the two supporting graphs: $G_2(A)$ and $G_2(B)$.

For a binary sequence X of length n, the *characteristic set* of X is given by

$$\mathcal{I}_X := \{t \in \mathbb{Z}_n : X(t) = 1\}.$$

A cyclic shift of X by τ corresponds to a translation of $\mathcal{I}_X$ by τ in $\mathbb{Z}_n$, that is, $\mathcal{I}_{\mathcal{R}^\tau X} = \mathcal{I}_X + \tau$. Let n, k, Δ be integers with $0 < k < n$ and $0 \le \Delta < n$. Given two distinct binary sequences $X, Y \in \mathcal{S}(n, k)$, it is easy to see that $H_\Delta(X, Y) \le 1$ if and only if $G_\Delta(\mathcal{I}_X)$ and $G_\Delta(\mathcal{I}_Y)$ are edge-disjoint.

Definition 4 Let $\mathcal{P} = \{P_1, P_2, \ldots, P_N\}$ be a set of k-subsets of $\mathbb{Z}_n$. We say $\mathcal{P}$ is a (k, Δ)-*packing* of K_n if $G_\Delta(P_i)$ and $G_\Delta(P_j)$ are edge-disjoint whenever $i \ne j$.

The following follows directly from definitions.

Proposition 2 *Let n, k, Δ be integers with $0 < k < n$ and $0 \le \Delta < n$. There exists a code $\mathcal{C} \in PCAC_\Delta(n, k)$ with $|\mathcal{C}| = N$ if and only if K_n has a (k, Δ)-packing $\mathcal{P} = \{P_1, P_2, \ldots, P_N\}$. More precisely, $\mathcal{P} = \{\mathcal{I}_X : X \in \mathcal{C}\}$.*

A (k, Δ)-packing $\mathcal{P}$ of K_n is said to be *maximum* if the size of $\mathcal{P}$ is maximum. That is, a maximum (k, Δ)-packing of K_n is equivalent to an optimal PCAC_Δ of length n and weight k.

3.3 Disjoint difference set

Definition 5 An (n, k, r)-*disjoint difference set* (*DDS*) is a family $\{B_1, B_2, \ldots, B_r\}$ of k-subsets of $\mathbb{Z}_n$ such that among the differences $\{x - y : x, y \in B_i, x \neq y, 1 \leq i \leq r\}$ each nonzero element $g \in \mathbb{Z}_n$ occurs at most once.

A necessary condition for the existence of an (n, k, r)-DDS is

$$n \geq rk(k-1) + 1. \tag{5}$$

An (n, k, r)-DDS is called as an (n, k)-*difference family* (DF) if the equality in (5) holds. That is, an (n, k)-DF is an $(n, k, \frac{n-1}{k(k-1)})$-DDS.

Let $\{B_1, B_2, \ldots, B_r\}$ be an (n, k, r)-DDS. It is easy to check that for any $\Delta, t, t' \geq 0$, the two cliques C_{B_i+t} and $C_{B_i+t'}$ have no common edges whenever $t \neq t'$, and the two supporting graphs $G_\Delta(B_i + t)$ and $G_\Delta(B_j + t')$ are edge-disjoint whenever $i \neq j$. Hence, we have the following proposition.

Proposition 3 *Let* $\{B_1, B_2, \ldots, B_r\}$ *be an* (n, k, r)*-DDS. For* $0 \leq \Delta < n$*, there exists a* (k, Δ)*-packing of* K_n *with size* $r \left\lfloor \frac{n}{\Delta+1} \right\rfloor$.

Proof By the observation above, the set of supporting graphs $G_\Delta(B_i + t)$ for $i = 1, 2, \ldots, r$ and $t = 0, (\Delta + 1), 2(\Delta + 1), \ldots, (\lfloor \frac{n}{\Delta+1} \rfloor - 1)(\Delta + 1)$ will form a (k, Δ)-packing of K_n. This concludes the proof. □

Combining Propositions 1, 2 and 3, we conclude that

Theorem 2 *If there exists an* (n, k, r)*-DDS, then for* $0 \leq \Delta < n$*, there exists an* $(n, k; \Delta)$*-UI sequence set of size*

$$N = r \left\lfloor \frac{n}{\Delta + 1} \right\rfloor. \tag{6}$$

In order to obtain (n, k, r)-DDSs, we revisit a useful combinatorial structure called difference triangle sets.

Definition 6 A *normalized* (r, k)*-difference triangle set* (*DTS* for short) is a family $\{B_1, B_2, \ldots, B_r\}$, where $B_i = \{b_{i0}, b_{i1}, \ldots, b_{ik}\}$, $1 \leq i \leq r$, are sets of integers such that $0 = b_{i0} < b_{i1} < \cdots < b_{ik}$, for all i, and such that the differences $b_{ij'} - b_{ij}$ with $1 \leq i \leq r$ and $0 \leq j < j' \leq k$ are all distinct. The *scope* of an (r, k)-DTS is the maximum integer among $\{b_{1k}, b_{2k}, \ldots, b_{rk}\}$.

It is known that a DDS can be obtained from a DTS.

Theorem 3 [19] *An* $(r, k-1)$*-DTS of scope* m *is an* (n, k, r)*-DDS for all* $n \geq 2m + 1$.

Please refer to [2,3,7,8,13,19] for more information on DDSs and DTSs. Note that a DDS is also named as a *difference packing (DP)* in literature.

3.4 An example

We use an example to illustrate our idea. Suppose that we aim to construct a (19, 3; 5)-UI set of size as large as possible. The first step is to find a (19, 3, 3)-DDS : $B_1 = \{0, 4, 5\}$, $B_2 =$

$\{0, 6, 8\}$, $B_3 = \{0, 7, 10\}$. Note that $\{B_1, B_2, B_3\}$ forms a difference family. By Proposition 3, we have a $(3, 5)$-packing of K_{19} as follows:

$$\begin{aligned}&\text{From } B_1 : \{0, 4, 5\}, \{6, 10, 11\}, \{12, 16, 17\},\\ &\text{From } B_2 : \{0, 6, 8\}, \{6, 12, 14\}, \{12, 18, 1\},\\ &\text{From } B_3 : \{0, 7, 10\}, \{6, 13, 16\}, \{12, 0, 3\}.\end{aligned}$$

Therefore, by Propositions 1 and 2, the 9 desired sequences are listed below.

$$\begin{aligned}B_1 &: 1000110000000000000,\ 0000001000110000000,\ 0000000000001000110,\\ B_2 &: 1000001010000000000,\ 0000001000001010000,\ 0100000000001000001,\\ B_3 &: 1000000100100000000,\ 0000001000000100100,\ 1001000000001000000.\end{aligned}$$

Let us consider a network of 9 potential users with the constraint that at most 3 of them are active at the same time and the maximum relative shift is 5. Then above example (PCAC approach) provides a solution with sequence length $n = 19$. If we consider TDMA approach, the length of sequences must be larger than $9 \times 5 = 45$. If we consider GF (or RS code) approach, by taking $k = 3$, $\Delta = 5$ and $N \geq 9$ into Theorem 1, we have $m \geq 2$ and $q \geq 3$, and thus $n \geq (5 + 1) \times 3^2 = 54$. This indicates that applying PCAC approach is more efficient than the other two methods. We will study this phenomenon in more details in the subsequent section.

3.5 Remarks

It must be noted that the connection in Proposition 3 is an old fashion. In fact, such a link is widely used to construct a block design from a difference family, see [7,19]. However, it is new to connect it with CAC or protocol sequences. If we let $D(B)$ denote the set of differences of any two elements in a set $B \subset \mathbb{Z}_n$, then any two sequences X and Y in a CAC have the property that $D(\mathcal{I}_X) \cap D(\mathcal{I}_Y) = \emptyset$. Since the quantity of sequences is what counts here, a good (or optimal) CAC is designed to make sure each $|D(\mathcal{I}_X)|$ is as small as possible, which is different from the demand of a difference family or a disjoint difference set.

4 New construction of UI sequence sets

In this section, we first construct a few families of UI sequence sets by means of disjoint difference sets, and then compare them with the UI sequence sets produced in Sect. 2.

Singer [22] constructed $(q^2 + q + 1, q + 1, 1)$-DDS, and Bose [1] constructed $(q^2 - 1, q, 1)$-DDS, where q is a prime power. With these DDSs and a construction of Colbourn–Bolbourn [10], Chen–Fan–Jin [7] proposed two infinite families of disjoint difference sets.

Theorem 4 [7] *Let q be a prime power.*

(a) *There exists an $\big(r(q^2 + q + 1), q + 1, r\big)$-DDS for any prime $r > q$.*

(b) *There exists an $\big(r(q^2 - 1), q, r\big)$-DDS for any prime $r \geq q$.*

By Theorem 2, we have the following result.

Theorem 5 *Let q be a prime power.*

(a) *For $r = 1$ or $r > q$ is a prime, there exists an $\big(r(q^2 + q + 1), q + 1; \Delta\big)$-UI sequence set with size*

$$N = r \left\lfloor \frac{r(q^2 + q + 1)}{\Delta + 1} \right\rfloor.$$

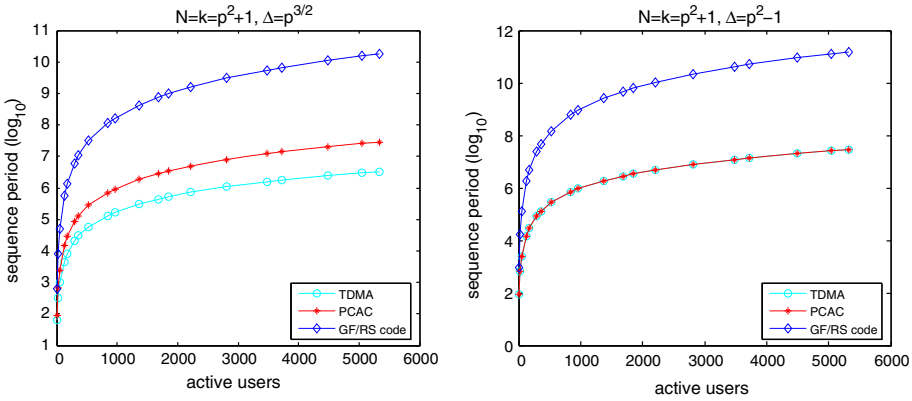

Fig. 3 $(n, k; (k-1)^{3/4})$-UI and $(n, k; (k-2))$-UI sequence sets for $k = p^2 + 1$, where p is a prime between 3 and 73

Table 1 Comparison of three approaches

	Potential users	Sequence period	Active users	
PCAC	$r\left\lfloor \frac{r(q^2+q+1)}{\Delta+1} \right\rfloor$	$r(q^2+q+1)$	$q+1$	q is a prime power and $r = 1$ or $r > q$ is a prime
	$r\left\lfloor \frac{r(q^2-1)}{\Delta+1} \right\rfloor$	$r(q^2-1)$	q	q is a prime power and $r = 1$ or $r \geq q$ is a prime
GF RS code	q^m	$q^2(\Delta+1)$	k	q is a prime power and $q \geq (k-1)(m-1)+1$
TDMA	k	$k(\Delta+1)$	k	

(b) *For $r = 1$ or $r \geq q$ is a prime, there exists an $\left(r(q^2-1), q; \Delta\right)$-UI sequence set with size*

$$N = r\left\lfloor \frac{r(q^2-1)}{\Delta+1} \right\rfloor.$$

Theorem 5 provides a new method to construct $(n, k; \Delta)$-UI sequence sets for some particular n. We now investigate the properties of the three constructions: PCAC, TDMA and GF (or RS code) methods. See the following chart for the comparisons.

We first consider the case that all potential users can be active at the same time; see Fig. 3 for examples. For simple illustration, we fix the number of active users (or potential users) to be $k = p^2 + 1$ and $\Delta = p^{3/2}$ or $p^2 - 1$, where p is a prime. In order to attain $p^2 + 1$ active users, by Table 1, the sequence period provided by PCAC approach is at least $p^4 + p^2 + 1$ (i.e., $r = 1$ of Case (a)), and by GF/RS code approach is at least $(p^2+1)^2(\Delta+1)$ (since the parameter $q \geq p^2 + 1$ in this case). Note that the curves of TDMA and PCAC approaches overlap in Fig. 3 (right) since the original sequence periods provided by them differ by 1 ($p^4 + p^2 + 1$ for PCAC and $p^4 + p^2$ for TDMA).

The result reveals that when the number of potential users is almost equal to the maximum number of active users in a system, the TDMA approach has a better performance, where the difference between it with PCAC approach is getting smaller as Δ approaches k.

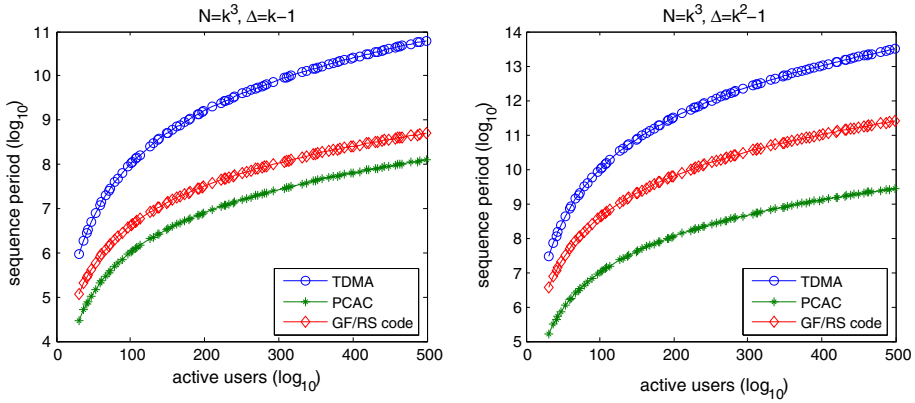

Fig. 4 $(n, k; k-1)$-UI and $(n, k; k^2-1)$-UI sequence sets with size k^3, where k is a prime between 31 and 499

In practice, however, the number of potential users is much larger than the maximum number of active ones. Consider the following two cases, shown in Fig. 4: The number of active users k is set to be a prime p, the numbers of potential users is p^3, and Δ is $p-1$ or p^2-1. For PCAC approach, we adopt the Case (b) by letting $r = p$ in the case of $\Delta = p-1$, and r be the smallest prime larger than $p^{3/2}$ in the case of $\Delta = p^2-1$. By Table 1, the period of sequences with respect to PCAC (resp. GF/RS code and TDMA) approach is approximately p^3 (resp. $4p^3$ and p^4) in the first case where $\Delta = k^2$, and approximately $p^{7/2}$ (resp. $4p^4$ and p^5) in the second one, where $\Delta = k^3$. Note that the parameter m in GF/RS code approach is taken to be 3 to attain the corresponding code size. One can see that in these two cases, the PCAC approach is much more efficient than the other schemes.

Roughly speaking, by Table 1, the PCAC approach provides an $(n, k; \Delta)$-UI sequence set of length $O(k\sqrt{N\Delta})$, while the lengths of sequences in the TDMA and GF/RS code approaches are respectively $O(N\Delta)$ and $O(\Delta k^2 m^2)$, where N is the code size. Therefore, the PCAC is more efficient under the condition:

$$k^2 m^4 \Delta > N > \frac{k^2}{\Delta}.$$

5 Partially conflict-avoiding codes of small weight

In this section, we investigate optimal partially conflict-avoiding codes. The main technique is to view an optimal PCAC_Δ of length n as a maximum packing of K_n. By Lemma 1, we only need to consider $\Delta < \lfloor \frac{n}{2} \rfloor$.

5.1 Weight $k = 2$

Let i, j be the two endpoints of an edge e in K_n. The *difference* of e, denoted by $d(e)$, is defined as the smallest nonzero integer t such that

$$i + t \equiv j \pmod{n} \text{ or } j + t \equiv i \pmod{n}.$$

Note that $1 \le d(e) \le \frac{n}{2}$ for any edge e in K_n. Note also that in K_n there are exactly n edges of difference t for each $1 \le t < \frac{n}{2}$, and there are exactly $\frac{n}{2}$ edges of difference $\frac{n}{2}$ provided that n is even. We say an edge e is *exceptional* if $d(e) = \frac{n}{2}$ and is *normal* otherwise.

Lemma 2 *For $0 \le \Delta < \lfloor \frac{n}{2} \rfloor$, the maximum size of a $(2, \Delta)$-packing of K_n is $\frac{n-1}{2}\lfloor \frac{n}{\Delta+1} \rfloor$ if n is odd, and $(\frac{n}{2}-1)\lfloor \frac{n}{\Delta+1} \rfloor + \lfloor \frac{n}{2\Delta+2} \rfloor$ if n is even.*

Proof Assume that $\mathcal{P}$ is a maximum packing. For each $A \in \mathcal{P}$, the supporting graph G_A is consist of $\Delta+1$ edges with the same difference d. Then the difference d could produce at most $\lfloor \frac{n}{\Delta+1} \rfloor$ supporting graphs if $d < \frac{n}{2}$ or at most $\lfloor \frac{n/2}{\Delta+1} \rfloor$ supporting graphs if $d = \frac{n}{2}$. Conversely, the construction is straightforward. Hence the result follows. □

Combining Lemma 2 and Proposition 2 together with the fact that $M(n, 2) = \lfloor \frac{n}{2} \rfloor$, we have:

Theorem 6 *Let n, Δ be integers with $0 \le \Delta < n$. Then*

$$M_\Delta(n,2) = \begin{cases} \frac{n-1}{2}\lfloor \frac{n}{\Delta+1} \rfloor & \text{if } n \text{ is odd and } \Delta \le \frac{n-3}{2}; \\ (\frac{n}{2}-1)\lfloor \frac{n}{\Delta+1} \rfloor + \lfloor \frac{n}{2\Delta+2} \rfloor & \text{if } n \text{ is even and } \Delta \le \frac{n-2}{2}; \\ \lfloor \frac{n}{2} \rfloor & \text{otherwise.} \end{cases}$$

5.2 Weight $k = 3$

Let A be a 3-subset of $\mathbb{Z}_n$ and Δ be an integer with $0 \le \Delta < \frac{n}{2}$. If two of the three edges in C_A have the same difference, then the number of edges in $G_\Delta(A)$, denoted by $\|G_\Delta(A)\|$, can be determined by the two distinct differences. For example, let $n = 8$. There are seven edges (four of difference 1 and three of difference 2) in $G_2(\{0, 1, 2\})$, and eight edges (five of difference 2 and three of difference 4) in $G_2(\{3, 5, 7\})$, see Fig. 2. We characterize this phenomenon below.

Lemma 3 *Let A be a 3-subset of $\mathbb{Z}_n$ and Δ be an integer with $0 \le \Delta < \lfloor \frac{n}{2} \rfloor$. If there exist two edges in C_A with the same difference d such that $d \ne \frac{n}{3}$, then*

$$\|G_\Delta(A)\| = \begin{cases} 2\Delta + 2 + d & \text{if } d \le \Delta, \\ 3(\Delta+1) & \text{if } d > \Delta, \end{cases}$$

where $\|G_\Delta(A)\|$ is the number of edges in $G_\Delta(A)$.

Proof Assume $A = \{i, j, k\}$ and $i - j \equiv j - k \equiv d \pmod n$. Let $E_1 = \bigcup_{\tau=0}^{\Delta} \{i+\tau, j+\tau\}$, $E_2 = \bigcup_{\tau=0}^{\Delta} \{j+\tau, k+\tau\}$ and $E_3 = \bigcup_{\tau=0}^{\Delta} \{i+\tau, k+\tau\}$ be the sets of edges in $G_\Delta(A)$. It is easy to see that $E_1 \cap E_2$ is empty if $d > \Delta$ and is equal to $\{i, j\} \cup \cdots \cup \{i+\Delta-d, j+\Delta-d\}$ if $d \le \Delta$. That is, there are $\Delta - d + 1$ repeated edges if $d \le \Delta$. Since $d \ne \frac{n}{3}$, $E_1 \cap E_3 = \emptyset$ and $E_2 \cap E_3 = \emptyset$. This completes the proof. □

We note here that if $d = \frac{n}{3}$ in above lemma, then $\|G_\Delta(A)\| = 3(\Delta+1)$ if $\frac{n}{3} > \Delta$ and $\|G_\Delta(A)\| = n$ if $\frac{n}{3} \le \Delta$. We have the following result.

Lemma 4 *Given a maximum $(3, \Delta)$-packing $\mathcal{P}$ of K_n, where n and Δ are positive integers with $\Delta < \lfloor \frac{n}{2} \rfloor$. Then*

$$|\mathcal{P}| < \frac{n(n-1)}{6(\Delta+1)} + \frac{2\ln 2 - 1}{3}n + \frac{n}{3(\Delta+1)}. \tag{7}$$

Proof We only consider $3 \nmid n$ because the case $3|n$ can be dealt with in the same way. For $d = 1, \ldots, \Delta$, let $T_d \subset \mathcal{P}$ be the collection of 3-subsets A such that in C_A, some two edges are of the same difference d. The cardinality of T_d is denoted by t_d. By Lemma 3, each T_d

corresponds to $(2\Delta+2+d)t_d$ edges and each of the remaining 3-subsets (not in some T_d) corresponds to $3(\Delta+1)$ edges. Furthermore, every $G_\Delta(A)$ for $A \in T_d$ contains exactly $\Delta+d+1$ edges with difference d, so $t_d \le \frac{n}{\Delta+d+1}$. Then,

$$\begin{aligned} M &\le t_1+t_2+\cdots+t_\Delta+\frac{\binom{n}{2}-((2\Delta+3)t_1+(2\Delta+4)t_2+\cdots+(3\Delta+2)t_\Delta)}{3(\Delta+1)} \\ &= \frac{n(n-1)}{6(\Delta+1)}+\frac{\Delta t_1+(\Delta-1)t_2+\cdots+t_\Delta}{3(\Delta+1)} \\ &\le \frac{n(n-1)}{6(\Delta+1)}+\frac{n}{3(\Delta+1)}\sum_{d=1}^{\Delta}\frac{\Delta+1-d}{\Delta+1+d}. \end{aligned}$$

Consider the last summation, we have

$$\begin{aligned} \sum_{d=1}^{\Delta}\frac{\Delta+1-d}{\Delta+1+d} &\le \int_0^\Delta\left(\frac{\Delta+1-x}{\Delta+1+x}\right)\mathrm{d}x=\int_0^\Delta\left(\frac{2(\Delta+1)}{\Delta+1+x}-1\right)\mathrm{d}x \\ &= 2(\Delta+1)\ln\left(\frac{2\Delta+1}{\Delta+1}\right)-\Delta \le 2(\Delta+1)\ln 2-\Delta, \end{aligned}$$

and thus the result follows. □

The following result on difference triangle sets can be constructed from *Skolem sequences* [23] and *hooked Skolem sequences* [17].

Theorem 7 [17,23] *There exists a* $(r,2)$*-DTS with scope* $3r$ *whenever* $r \equiv 0,1$ *(mod 4), and scope* $3r+1$ *whenever* $r \equiv 2,3$ *(mod 4).*

By Theorem 3, there exists an $(n,3,r)$-DDS for all $n \ge 6r+1$ whenever $r \equiv 0,1 \pmod 4$, and $n \ge 6r+3$ whenever $r \equiv 2,3 \pmod 4$. Applying Proposition 3 we obtain the following result.

Lemma 5 *Let* n, Δ *be positive integers such that* $\Delta < \lfloor \frac{n}{2} \rfloor$*. There exists a* $(3,\Delta)$*-packing* $\mathcal{P}$ *of* K_n *with*

$$|\mathcal{P}| = \left\lfloor \frac{n-1}{6} \right\rfloor \left\lfloor \frac{n}{\Delta+1} \right\rfloor.$$

The following result can be obtained by Proposition 2 together with Lemmas 4 and 5.

Theorem 8 *Let* n, Δ *be positive integers such that* $\Delta < \lfloor \frac{n}{2} \rfloor$*. Then*

$$\left\lfloor \frac{n-1}{6} \right\rfloor \left\lfloor \frac{n}{\Delta+1} \right\rfloor \le M_\Delta(n,3) \le \frac{n(n-1)}{6(\Delta+1)}+\frac{2\ln 2-1}{3}n+\frac{n}{3(\Delta+1)}.$$

Table 2 lists some upper and lower bounds of $M_\Delta(n,3)$ for $\Delta=\sqrt{n}$, where $n=200t$ for $t=1,2,\ldots,18$. One can imagine that the larger the value n, the smaller the gap between the two bounds with respect to n. Generally speaking, if Δ is fixed (a constant or a function of n), then the code size obtained by disjoint difference sets approximately attains the theoretical upper bound $O(\frac{n^2}{6\Delta})$ as $n \to \infty$.

Table 2 Upper and lower bounds on $M_{\sqrt{n}}(n, 3)$

n	200	400	600	800	1,000	1,200	1,400	1,600	1,800
Upper bound	442	1,273	2,357	3,647	5,114	6,739	8,509	10,413	12,441
Lower bound	429	1,254	2,277	3,591	4,980	6,567	8,388	10,374	12,259
n	2,000	2,200	2,400	2,600	2,800	3,000	3,200	3,400	3,600
Upper bound	14,588	16,846	19,212	21,679	24,244	26,904	29,655	32,494	35,419
Lower bound	14,319	16,470	19,152	21,650	23,766	26,447	29,315	32,262	35,341

Table 3 Some lower bounds on $M_{\sqrt{n}}(n, k)$ for $k = 4, 5, 6, 7$

n	13	37	61	73	97	109	157	181	193	229	241	277
$M_{\sqrt{n}}(n, 4)$	2	15	30	42	64	81	143	180	192	266	280	345
n	41	61	101	181	241	281	401	421	461	521	541	601
$M_{\sqrt{n}}(n, 5)$	10	18	45	108	168	210	380	399	460	546	594	690
n	31	151	181	211	241	271	331	421	541	571	601	631
$M_{\sqrt{n}}(n, 6)$	4	55	72	91	112	135	187	266	396	418	460	504
n	337	379	421	463	547	631	673	757	883	967	1,009	1,051
$M_{\sqrt{n}}(n, 7)$	136	162	190	220	286	360	384	468	588	690	720	775

5.3 Weight $k = 4, 5, 6, 7$

Here are some difference family results on $k = 4, 5, 6, 7$.

Theorem 9 *[4–6]*

(i) *For any prime* $p \equiv 1$ *(mod* 12*) there exists a* $(p, 4)$*-DF.*
(ii) *For any prime* $p \equiv 1$ *(mod* 20*) there exists a* $(p, 5)$*-DF.*
(iii) *For any prime* $p \equiv 1$ *(mod* 30*) there exists a* $(p, 6)$*-DF with one exception of* $p = 61$.
(iv) *Let* $p \equiv 1$ *(mod* 42*) be a prime and* $p \neq 43, 127, 211$. *Then there exists a* $(p, 7)$*-DF whenever* $(-3)^{\frac{p-1}{14}} \neq 1$ *in* $\mathbb{Z}_p$ *or* $p < 261239791$ *or* $p > 1.236597 \times 10^{13}$.

Since an (n, k)-DF is an $\left(n, k, \frac{n-1}{k(k-1)}\right)$-DDS, the corresponding PCAC_Δs are obtained directly by Propositions 2 and 3. In Table 3 we consider $\Delta = \sqrt{n}$ and list some examples of small n which satisfy conditions in Theorem 9. We note here that more PCAC_Δs, especially for small weights, can be produced by a recursive construction of DTSs with minimum scope [8].

6 Concluding remarks

In this paper we construct an infinite number of new partially UI sequence sets by means of PCAC_Δ or disjoint difference sets. For some particular n, we are able to obtain an asymptotically optimal PCAC_Δ of length n and weight three.

Acknowledgments The work partially supported by Research Grants Council of the Hong Kong Special Administrative Region under Project 414012 (Y.-H. Lo and W. S. Wong), and the National Science Council under Grants 100-2115-M-009-005-MY3 (H.-L. Fu).

References

1. Bose R.C.: An affine analogue of Singer's theorem. Ind. Math. Soc. **6**, 1–5 (1942).
2. Chee Y.M., Colbourn C.J.: Constructions for difference triangle sets. IEEE Trans. Inf. Theory **43**(4), 1346–1349 (1997).
3. Chen Z.: Further results on difference triangle sets. IEEE Trans. Inf. Theory **40**(4), 1268–1270 (1994).
4. Chen K., Zhu L.: Existence of $(q, 6, 1)$ difference families with q a prime power. Des. Codes Cryptogr. **15**, 167–173 (1998).
5. Chen K., Zhu L.: Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. J. Comb. Des. **7**(1), 21–30 (1999).
6. Chen K., Zhu L.: Existence of $(q, 7, 1)$ difference families with q a prime power and $k = 4, 5$. J. Comb. Des. **10**(2), 126–138 (2002).
7. Chen Z., Fan P., Jin F.: Disjoint difference sets, difference triangle sets, and related codes. IEEE Trans. Inf. Theory **38**(2), 518–522 (1992).
8. Chu W., Colbourn C.J., Golomb S.W.: A recursive construction for regular difference triangle sets. SIAM J. Discret. Math. **18**(4), 741–748 (2005).
9. Chlamtac I., Faragó A.: Making transmission schedules immune to topology changes in multi-hop packet radio networks. IEEE/ACM Trans. Netw. **2**(1), 23–29 (1994).
10. Colbourn M.J., Colcourn C.J.: Recursive constructions for cyclic block designs. J. Stat. Plann. Infer. **10**, 97–103 (1984).
11. Fu H.-L., Lin Y.-H., Mishima M.: Optimal conflict-avoiding codes of even length and weight 3. IEEE Trans. Inf. Theory **56**(11), 5747–5756 (2010).
12. Fu H.-L., Lo Y.-H., Shum K.W.: Optimal conflict-avoiding codes of odd length and weight three. Des. Codes Cryptogr. **72**(2), 289–309 (2014).
13. Ling A.C.H.: Difference triangle sets from affine planes. IEEE Trans. Inf. Theory **48**(8), 2399–2401 (2002).
14. Levenshtein V.I., Tonchev V.D.: Optimal conflict-avoiding codes for three active users. In: Proceedings of IEEE International Symposium on Information Theory, Adelaide, Australia, pp. 535–537 (2005).
15. Massey J.L., Mathys P.: The collision channel without feedback. IEEE Trans. Inf. Theory **31**(2), 192–204 (1985).
16. Momihara K., Müller M., Satoh J., Jimbo M.: Constant weight conflict-avoiding codes. SIAM J. Discret. Math. **21**(4), 959–979 (2007).
17. O'keefe E.S.: Verification of a conjecture of Th. Skolem. Math. Stand. **9** 80–82 (1961).
18. Rentel C.H., Kunz T.: Reed-solomon and hermitian code-based scheduling protocols for wireless ad hoc networks. In: The 4th International Conference on Ad Hoc and Wireless Networks, Cancun, Mexico (2005).
19. Shearer J.B.: Difference triangle sets. In: Colbourn C.J., Dinitz J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn. Chapman and Hall/CRC, Boca Raton (2007)
20. Shum K.W., Wong W.S., Chen C.S.: A general upper bound on the size of constant-weight conflict-avoiding codes. IEEE Trans. Inf. Theory **56**(7), 3265–3276 (2010).
21. Shum K.W., Wong W.S., Sung C.W., Chen C.S.: Design and construction of protocol sequences: shift invariance and user irrepressibility. In: IEEE International Symposium on Information Theory, Seoul, Korea, pp. 1368–1372 (2009).
22. Singer J.: A theorem in finite projective geometry and some applications to number theory. AMS Trans. **43**, 377–385 (1938).
23. Skolem T.: On certain distributions of integers in pairs with given differences. Math. Stand. **5**, 57–58 (1957).
24. Wong W.S.: New protocol sequences for random access channels without feedback. IEEE Trans. Inf. Theory **53**(6), 2060–2071 (2007).
25. Wong W.S.: Transmission sequence design and allocation for wide area ad hoc networks. IEEE Trans. Veh. Technol. **63**(2), 869–878 (2014).
26. Wu Y., Shum K.W., Wong W.S., Su Q., Shen L.-F.: Deterministic channel access using quasi-random protocol sequences. IEEE Trans. Veh. Technol. **63**(3), 1467–1479 (2014).