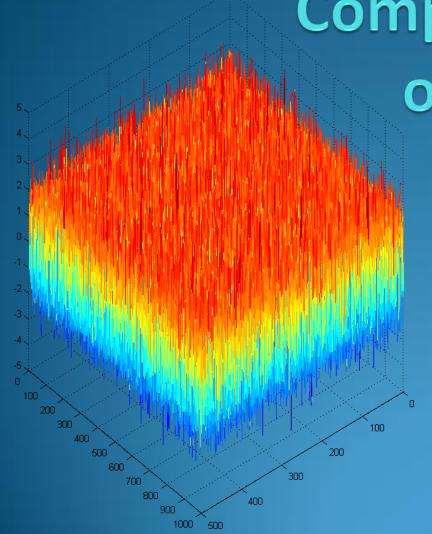


M. Soltanalian & P. Stoica, Sept. 2011.





Clarifications:

- Sequences: of different lengths, of different dimension sizes, of different alphabets.
- Autocorrelation:

periodic
$$c_k = \sum_{l=1}^n \boldsymbol{x}(l) \ \boldsymbol{x}^*(l+k)_{mod \ n}, \ 0 \le k \le (n-1)$$
 aperiodic $r_k = \sum_{l=1}^{n-k} \boldsymbol{x}(l) \ \boldsymbol{x}^*(l+k) = r_{-k}^*, \ 0 \le k \le (n-1)$

<u>Good</u> correlation properties?

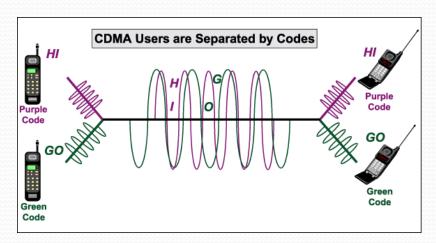
Small out-of-phase (i.e. $k \neq 0$) autocorrelation lags are required.



Applications

CDMA Communications

Active sensing (Radar, Sonar, etc.)



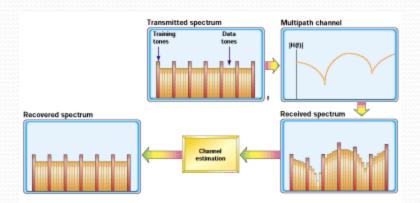




Applications

Channel estimation

Synchronization





• Data hiding, ultra-wideband (UWB) communications, synthesis of orthogonal matrices for source coding and complementary coding, . . .



Why computational design?

• Metrics:

$$\begin{aligned} & peak \ sidelobe \ level & \qquad & \text{PSL} = \max\{|r_k|\}_{k=1}^{n-1}, \\ & \text{integrated sidelobe level} & \qquad & \text{ISL} = \sum_{k=1}^{n-1} |r_k|^2, \\ & \qquad & \text{merit factor} & \qquad & \text{MF} = \frac{|r_0|^2}{2\sum_{k=1}^{n-1} |r_k|^2} = \frac{E^2}{2\ \text{ISL}}. \end{aligned}$$



Complementary sets of sequences:

A set $S = \{x_1, x_2, \dots, x_m\}$ containing m sequences of length n is called a set of (periodically) complementary sequences when the (periodic) autocorrelation values of $\{x_k\}_{k=1}^m$ sum up to zero at any out-of-phase lag. This property can be formulated as

$$\sum_{l=1}^{m} c_{l,k} = 0, \quad \forall \ 1 \le k \le (n-1)$$

where $c_{l,k}$ represents the k^{th} (periodic) autocorrelation lag of x_l .



Definition 1. The twisted product of two vectors x and y (both in $\mathbb{C}^{n\times 1}$) is defined as

$$m{x} \circlearrowleft m{y}^H = \left(egin{array}{cccc} m{x}(1)m{y}^*(1) & m{x}(2)m{y}^*(2) & \cdots & m{x}(n)m{y}^*(n) \\ m{x}(1)m{y}^*(2) & m{x}(2)m{y}^*(3) & \cdots & m{x}(n)m{y}^*(1) \\ dots & dots & \ddots & dots \\ m{x}(1)m{y}^*(n) & m{x}(2)m{y}^*(1) & \cdots & m{x}(n)m{y}^*(n-1) \end{array}
ight)$$

where $\mathbf{x}(k)$ and $\mathbf{y}(k)$ are the k^{th} entries of \mathbf{x} and \mathbf{y} respectively. The **twisted rank-one approximation** of $\mathbf{Z} \in \mathbb{C}^{n \times n}$ is equal to $\mathbf{x} \circlearrowleft \mathbf{y}^H$ if and only if \mathbf{x} and \mathbf{y} are the solution of the optimization problem:

$$\min_{\boldsymbol{x}, \boldsymbol{y} \in \mathbb{C}^{n \times 1}} \|\boldsymbol{Z} - \boldsymbol{x} \circlearrowleft \boldsymbol{y}^H\|_F$$

• Note: there exists a known permutation matrix $P \in \mathbb{C}^{n^2 \times n^2}$ for which

$$||\mathbf{Z} - \mathbf{x} \circlearrowleft \mathbf{y}^{H}||_{F} = ||vec(\mathbf{Z}) - vec(\mathbf{x} \circlearrowleft \mathbf{y}^{H})||_{2}$$

$$= ||vec(\mathbf{Z}) - P|vec(\mathbf{x}\mathbf{y}^{H})||_{2}$$

$$= ||P^{T}vec(\mathbf{Z}) - vec(\mathbf{x}\mathbf{y}^{H})||_{2}$$

$$= ||\mathbf{Z}' - \mathbf{x}\mathbf{y}^{H}||_{F}$$

re-ordering function $\mathcal{F}(\cdot)$:

$$oldsymbol{Z}' = \mathcal{F}(oldsymbol{Z})$$



• Interestingly, the periodic autocorrelation of a vector x can be written as $(x \circlearrowright x^H)1$.

 \boldsymbol{x} is a perfect sequence with energy E \longleftrightarrow $(\boldsymbol{x} \circlearrowright \boldsymbol{x}^H)\mathbf{1} = E\boldsymbol{e}_1.$

$$S = \{ m{x}_1, m{x}_2, \cdots, m{x}_m \}$$
 a set of periodically complementary sequences
$$\sum_{k=1}^m (m{x}_k \ \circlearrowright \ m{x}_k^H) \mathbf{1} = \underline{E} m{e}_1.$$
 the total energy of $\{ m{x}_k \}_{k=1}^m$



• Suppose $X \in \mathbb{C}^{n \times n}$ is such that the sum of the entries of its rows is E for the first row and zero otherwise. Let us suppose that $\mathcal{F}(X)$ has $m \leq n$ nonzero positive eigenvalues and therefore that $\mathcal{F}(X)$ can be written as (for $x_k \neq 0$):

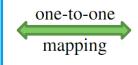
$$\mathcal{F}(oldsymbol{X}) = \sum_{k=1}^m oldsymbol{x}_k oldsymbol{x}_k^H$$

It follows that $oldsymbol{X} = \sum_{k=1}^m oldsymbol{x}_k \circlearrowleft oldsymbol{x}_k^H$ and as a result

$$oldsymbol{X} oldsymbol{1} = \sum_{k=1}^m (oldsymbol{x}_k \circlearrowleft oldsymbol{x}_k^H) oldsymbol{1} = E oldsymbol{e}_1$$

- The total energy E is distributed over m sequences $\{x_k\}_{k=1}^m$ that are complementary.
- The energy of $\{x_k\}_{k=1}^m$ is determined by the corresponding eigenvalues of $\mathcal{F}(X)$.
- Suppose the vector $\rho \in (\mathbb{R}^+ \cup \{0\})^{n \times 1}$ (whose entries sum up to E) represents the energy components of the sequences.

The solutions of the problem of designing sets of (periodically) complementary sequences when the desired energy for each sequence is given



convex set $\Gamma_{\mathcal{P}}(E)$ (\mathcal{P} stands for Periodic) of all matrices $\mathcal{F}(\boldsymbol{X}_0)$ such that $\boldsymbol{X}_0\mathbf{1}=E\boldsymbol{e}_1$

the set $\Lambda_{\mathcal{P}}(\rho)$ of all Hermitian matrices with the given vector of eigenvalues ρ



• The Aperiodic Autocorrelation For a sequence x of length n, the periodic autocorrelation lags of $x' = \begin{pmatrix} x \\ \mathbf{0}_{(n-1)\times 1} \end{pmatrix}$ are equal to the aperiodic autocorrelation lags of x for $0 \le k \le n-1$.

$$\Gamma_{\mathcal{P}}(E)$$
 replace with

 $\Gamma_{\mathcal{AP}}(E)$ (\mathcal{AP} stands for Aperiodic) which contains all matrices $\mathcal{F}(\boldsymbol{X}_0)$ such that

$$egin{cases} oldsymbol{X}_0 \in \mathbb{C}^{(2n-1) imes(2n-1)} \ oldsymbol{X}_0 oldsymbol{1} = E oldsymbol{e}_1 \ oldsymbol{\mathcal{F}}(oldsymbol{X}_0) \odot oldsymbol{\mathcal{M}} = \mathcal{F}(oldsymbol{X}_0) \end{cases}$$

where
$$\mathcal M$$
 is a masking matrix defined as $\mathcal M = \left(egin{array}{ccc} \mathbf 1_{n imes n} & \mathbf 0_{n imes (n-1)} \\ \mathbf 0_{(n-1) imes n} & \mathbf 0_{(n-1) imes (n-1)} \end{array}
ight).$



Let us also replace
$$\Lambda_{\mathcal{P}}(\boldsymbol{\rho})$$
 with $\Lambda_{\mathcal{AP}}(\boldsymbol{\rho}) = \Lambda_{\mathcal{P}}(\boldsymbol{\rho}')$ where $\boldsymbol{\rho}' = \begin{pmatrix} \boldsymbol{\rho} \\ \mathbf{0}_{(n-1)\times 1} \end{pmatrix}$.

• With the latter definitions, the intersection of the two sets $\Gamma_{\mathcal{AP}}(E)$ and $\Lambda_{\mathcal{AP}}(\boldsymbol{\rho})$ yields sets of vectors of length 2n-1 whose last n-1 entries are zero and whose first n entries form sequences with good aperiodic correlation properties.



- The main challenge of the algorithms is to tune the energy distribution over the sequences in each iteration while trying to preserve the mutual property of complementarity. This goal can be achieved using the idea of alternating projections.
- projection of an element of $\Lambda_{\mathcal{P}}(\boldsymbol{\rho})$ on $\Gamma_{\mathcal{P}}(E)$

Theorem. Let $X = Y^{\perp}$ be the optimal projection (for the matrix Frobenius norm) of $Y \in \mathbb{C}^{n \times n}$ on $\Gamma_{\mathcal{P}}(E)$. Then $\mathcal{F}^{-1}(X)$ can be obtained from $\mathcal{F}^{-1}(Y)$ by adding a fixed value to each row of $\mathcal{F}^{-1}(Y)$ such that $\mathcal{F}^{-1}(Y)1 = Ee_1$; more precisely,

$$\left[\mathcal{F}^{-1}(\boldsymbol{X}) \right]_{k,l} = \left[\mathcal{F}^{-1}(\boldsymbol{Y}) \right]_{k,l}$$

$$+ \frac{1}{n} \left(E \delta_{k-1} - \sum_{l'=1}^{n} \left[\mathcal{F}^{-1}(\boldsymbol{Y}) \right]_{k,l'} \right) .$$



• The projection of an element of $\Gamma_{\mathcal{P}}(E)$ on $\Lambda_{\mathcal{P}}(\rho)$:

$$X \longrightarrow X^{\perp}$$

 $X^{\perp} = UDU^{H}$ where $D = Diag(\rho)$ and U is a unitary matrix.

 $X = VD'V^H$ eigenvalue decomposition of X

Therefore, the problem of finding X^{\perp} is equivalent to

$$egin{array}{ll} \min & \|oldsymbol{V}oldsymbol{U}^H - oldsymbol{U}oldsymbol{U}^H\|_F^2 \ & ext{s.t.} & oldsymbol{U}oldsymbol{U}^H = oldsymbol{I} \end{array}$$

Theorem. Let $X \in \mathbb{C}^{n \times n}$ be a Hermitian matrix with the eigenvalue decomposition $VD'V^H$. Then the orthogonal projection of X (for the matrix Frobenius norm) on $\Lambda_{\mathcal{P}}(\rho)$ denoted by $Y = X^{\perp}$ can be obtained from X by replacing D' with D.



The ITROX- $\mathcal P$ Algorithm (for designing periodically complementary sets of sequences)

Step 0: Consider an initial point $X = \mathcal{F}(X_0) \in \Gamma_{\mathcal{P}}(E)$ for some X_0 that satisfies $X_0 \mathbf{1} = E \mathbf{e}_1$.

Step 1: Compute the eigenvalue decomposition $X = VD'V^H$ and find $Y = X^{\perp}$ (the orthogonal projection of X on $\Lambda_{\mathcal{P}}(\rho)$) by replacing D' with D (i.e. $Y = VDV^H$).

Step 2: Compute $X = Y^{\perp}$ by adding a fixed value to each row of $\mathcal{F}^{-1}(Y)$ such that $\mathcal{F}^{-1}(Y^{\perp})\mathbf{1} = Ee_1$.

Step 3: Repeat the projections in steps 1 and 2 until a stop criterion is satisfied, e.g. $\|\mathbf{X} - \mathbf{Y}\|_F < \epsilon$ for some given $\epsilon > 0$.



• projection on $\Gamma_{\mathcal{AP}}(E)$

Theorem. Let $X = Y^{\perp}$ be the optimal projection (for the matrix Frobenius norm) of $Y \in \mathbb{C}^{(2n-1)\times(2n-1)}$ on $\Gamma_{\mathcal{AP}}(E)$. Let w_k denote the number of ones in the k^{th} row of $\mathcal{F}^{-1}(\mathcal{M})$. Then

$$w_k = \sum_{l'=1}^{2n-1} \left[\mathcal{F}^{-1}(\mathcal{M}) \right]_{k,l'} = \begin{cases} n-k+1, & k \le n \\ k-n, & k > n \end{cases}$$

and the entries of $\mathcal{F}^{-1}(oldsymbol{X})$ are given by

$$[\mathcal{F}^{-1}(\boldsymbol{X})]_{k,l} = [\mathcal{F}^{-1}(\boldsymbol{Y})]_{k,l} + \frac{1}{w_k} \left(E\delta_{k-1} - \sum_{l'=1}^{2n-1} [\mathcal{F}^{-1}(\boldsymbol{\mathcal{M}} \odot \boldsymbol{Y})]_{k,l'} \right).$$

for all (k,l) such that $\left[\mathcal{F}^{-1}(\mathcal{M})\right]_{k,l}=1$ and zero otherwise.

• projection on $\Lambda_{\mathcal{AP}}(\rho)$ can be obtained as before since for any matrix $X \in \Gamma_{\mathcal{AP}}(E)$

$$oldsymbol{X} = \left(egin{array}{ccc} oldsymbol{V}_{n imes n} & oldsymbol{0}_{n imes (n-1)} \ oldsymbol{0}_{(n-1) imes n} & oldsymbol{I}_{n-1} \end{array}
ight) \left(egin{array}{ccc} oldsymbol{D}'_{n imes n} & oldsymbol{0}_{n imes (n-1)} \ oldsymbol{0}_{(n-1) imes n} & oldsymbol{0}_{(n-1) imes n} \end{array}
ight) \left(egin{array}{ccc} oldsymbol{V}^*_{n imes n} & oldsymbol{0}_{n imes (n-1)} \ oldsymbol{0}_{(n-1) imes n} & oldsymbol{I}_{n-1} \end{array}
ight)$$

where $VD'V^*$ is the eigenvalue decomposition of the $n \times n$ upper-left sub-matrix of X.



The ITROX- \mathcal{AP} algorithm (for designing complementary sets of sequences with good aperiodic correlation)

Step 0: Consider an initial point $X = \mathcal{F}(X_0) \in \Gamma_{\mathcal{AP}}(E)$ with nonzero entries only in its $n \times n$ upper-left sub-matrix and for which X_0 that satisfies $X_0 \mathbf{1} = E \mathbf{e}_1$.

Step 1: Compute the eigenvalue decomposition of X and find $Y = X^{\perp}$ (the orthogonal projection of X on $\Lambda(\rho)$) by replacing D' with D.

Step 2: Compute $X = Y^{\perp}$ by adding certain fixed values to some entires of Y and by making the others zero.

Step 3: Repeat the projections in steps 1 and 2 until a stop criterion is satisfied, e.g. $\|\mathbf{X} - \mathbf{Y}\|_F < \epsilon$ for some given $\epsilon > 0$.



ITROX: Convergence

Definition. Consider a pair of sets (T_1, T_2) . A pair of sets (C_1, C_2) where $C_1 \subseteq T_1$ and $C_2 \subseteq T_2$ is called an **attraction landscape** of (T_1, T_2) iff starting from any point in C_1 or C_2 , the alternating projections on T_1 and T_2 end up in the same element pair (c_1, c_2) $(c_1 \in C_1, c_2 \in C_2)$. Furthermore, for a pair of sets (T_1, T_2) , an attraction landscape (C_1, C_2) is said to be **complete** iff for any attraction landscape (C_1', C_2') such that $C_1 \subseteq C_1'$ and $C_2 \subseteq C_2'$, we have $C_1 = C_1'$ and $C_2 = C_2'$.

• Let X be the optimal projection of $Y \in \Lambda(\rho)$ on $\Gamma(E)$ and $\Delta X_0 = \mathcal{F}^{-1}(Y) - \mathcal{F}^{-1}(X)$. We have

$$\|\Delta X_0^{(s)}\|_F^2 = \sum_{k \in S \cup \{0\}} n \left| \frac{c_k^{(s)} - \delta_k E}{n} \right|^2$$
$$= \sum_{k \in S} n \left| \frac{c_k^{(s)}}{n} \right|^2 = \frac{1}{n} \text{ ISL}^{(s)}$$

This shows that the ISL metric is decreasing through the iterations of ITROX.



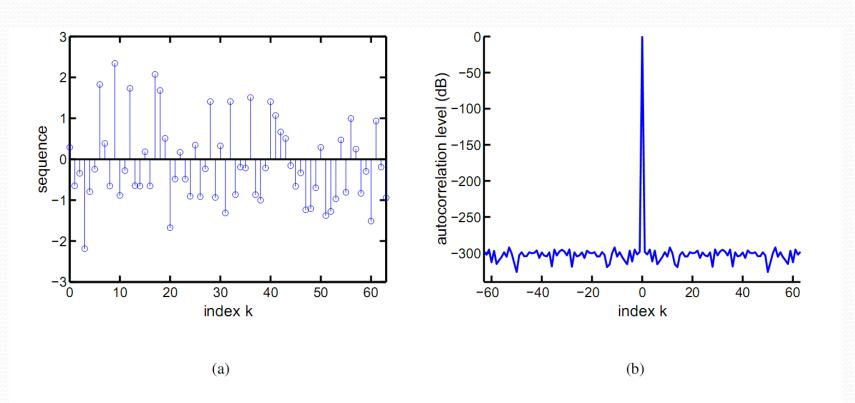


Fig. Design of a real-valued sequence of length 64 with good periodic autocorrelation. (a) and (b) depict the entries and the autocorrelation levels (in dB) of the sequence respectively.



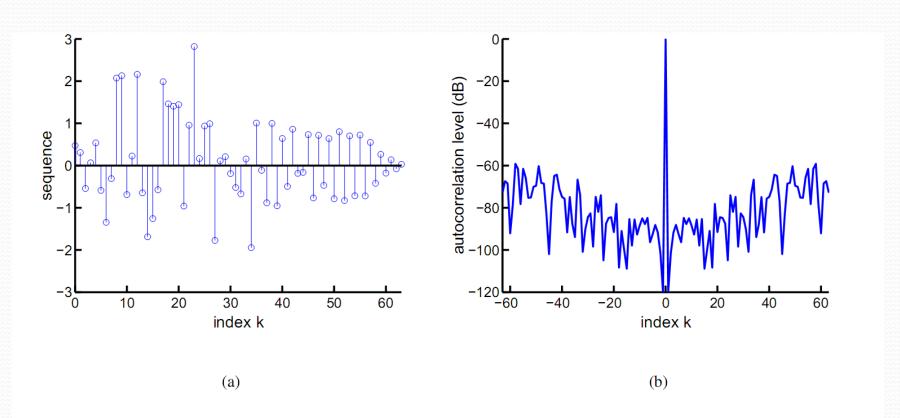


Fig. Design of a real-valued sequence (of length 64) with good aperiodic autocorrelation. (a) and (b) show the entries and the autocorrelation levels (in dB) of the sequence respectively.



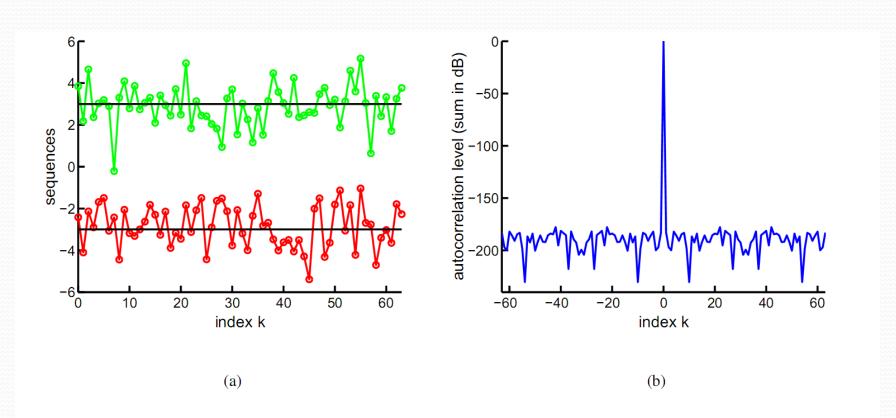


Fig. Design of a real-valued periodically complementary pair of sequences (both of length 64) using ITROX- \mathcal{P} . (a) plots of the sequences with a bias of +3 and -3 to distinguish the two sequences. (b) plot of the autocorrelation sum levels.



Constrained Sequence Design



Constrained Sequence Design:

Our goal here is to adapt the ITROX algorithms such that they can handle constrained alphabets. Namely, we are particularly interested in

binary
$$\{-1, +1\}$$
, integer \mathbb{Z} , unimodular $\{\zeta \in \mathbb{C} \mid |\zeta| = 1\}$ and root-of-unity $\{\zeta \in \mathbb{C} \mid \zeta^m = 1\}$ (for $m \geq 3$)

alphabets. To tackle such sequence design problems, we introduce a method which uses the idea of alternating projections but on a sequence of converging sets.



Definition . Consider a function $f(t,s): \mathbb{C} \times (\mathbb{N} \cup \{0\}) \to \mathbb{C}$; as an extension, for every matrix X let f(X,s) be a matrix such that $[f(X,s)]_{k,l} = f(X(k,l),s)$. We say that: (i) f is element-wisely monotonic iff for any $t \in \mathbb{C}$, both |f(t,s)| and $\arg(f(t,s))$ are monotonic in s. (ii) A set T is converging to a set T^{\dagger} under a function f iff for every $t \in T$,

$$\begin{cases} f(t,0) = t, \\ \lim_{s \to \infty} f(t,s) \in T^{\dagger} \end{cases}$$

and for every $t^{\dagger} \in T^{\dagger}$, there exists an element $t \in T$ such that

$$\lim_{s \to \infty} f(t, s) = t^{\dagger}. \tag{*}$$

(iii) The function f is identity iff for any $t \in T$ and $t^{\dagger} \in T^{\dagger}$ satisfying (*), t^{\dagger} is the closest element of T^{\dagger} to t, and (iv) the sequence of sets $\{T^{(s)}\}_{s=0}^{\infty}$ where $T^{(s)} = \{f(t,s) \mid t \in T\}$ is a sequence of converging sets.



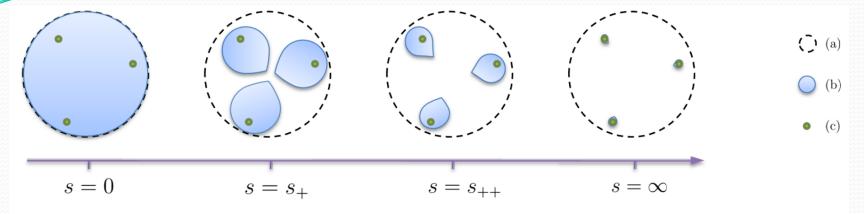


Fig. An example of a converging set. (a-c) show a (non-constrained) compact set T, the sets $T^{(s)}$, and entries of a (constrained) finite set T^{\dagger} respectively for $0 < s_+ < s_{++} < \infty$.

ullet examples of f for some constrained alphabets commonly used in sequence design:

$$(a) \ T = \mathbb{R} - \{0\}, \ T^{\dagger} = \{-1, 1\}:$$

$$f(t, s) = \operatorname{sgn}(t) \cdot |t|^{e^{-\nu s}}$$

$$(b) \ T = \mathbb{R}, \ T^{\dagger} = \mathbb{Z}:$$

$$f(t, s) = [t] + \{t\} \cdot e^{-\nu s}$$

$$(c) \ T = \mathbb{C} - \{0\}, \ T^{\dagger} = \{\zeta \in \mathbb{C} \mid |\zeta| = 1\}:$$

$$f(t, s) = |t|^{e^{-\nu s}} \cdot e^{j \operatorname{arg}(t)}$$

$$(d) \ T = \mathbb{C} - \{0\}, \ T^{\dagger} = \{\zeta \in \mathbb{C} \mid \zeta^m = 1\}:$$

$$f(t, s) = |t|^{e^{-\nu s}} \cdot e^{j \frac{2\pi}{m} \left(\left[\frac{m \operatorname{arg}(t)}{2\pi}\right] + \left\{\frac{m \operatorname{arg}(t)}{2\pi}\right\} \cdot e^{-\nu s}\right)}$$



We consider the following modification of typical alternating projections:

at the s^{th} step of the alternating projections, let $t_1^{(s)} \in T_1$ be the orthogonal projection of $t_2^{(s)} \in T_2$ on T_1 and let $t_1^{(s)} = f(t_1^{(s)}, s) \in T_1^{(s)}$. Now, instead of projecting $t_1^{(s)}$ on T_2 , we project $t_1^{(s)}$ on T_2 to obtain $t_2^{(s+1)}$.

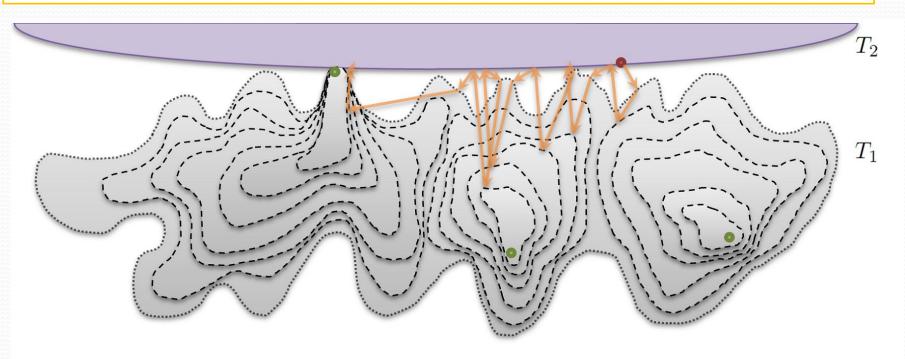


Fig. An illustration of the proposed modified alternating projections in which the algorithm converges to a good solution. The dashed-lines are used to represent the sets $T_1^{(s)}$ converging to $T_1^{\dagger} \subseteq T_1$ with 3 elements.



THE GENERAL FORM OF THE ITROX ALGORITHM FOR CONSTRAINED SEQUENCE DESIGN

Step 0: Consider an initial point $X = \mathcal{F}(X_0) \in \Gamma(E)$. Set the iteration counter (s) to zero.

Step 1: Compute the eigenvalue decomposition $X = VD'V^H$ and find $Y = X^{\perp}$ (the optimal projection of X on $\Lambda(\rho)$) by replacing D' with D (i.e. $Y = VDV^H$).

Step 2: Let $\Lambda(\rho)$ converge to Ω_X under some convenient function f as described in Definition (a set of examples are provided after the definition). Compute $\widetilde{Y} = f(Y, s)$.

Step 3: Compute $X = \widetilde{Y}^{\perp}$ by adding some fixed value to some given entries of \widetilde{Y} , make certain of them zero and leave the others unchanged (depending on the application).

Step 4: Increase the iteration counter (s) by one. Repeat the modified alternating projections (steps 1-3) if the stop criterion (e.g. either $\|\widetilde{\boldsymbol{Y}} - \boldsymbol{X}\|_F < \epsilon$ for some given $\epsilon > 0$ or $\widetilde{\boldsymbol{Y}}$ is sufficiently close to an element of $\Omega_{\boldsymbol{X}}$) is not satisfied.



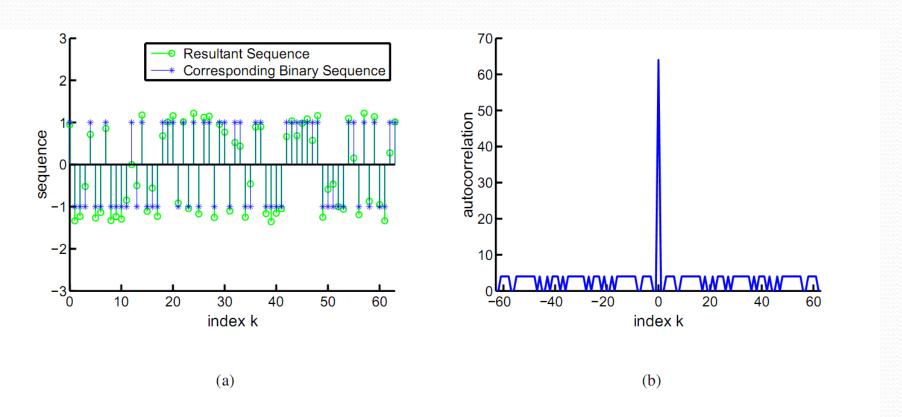


Fig. Design of a binary sequence of length 64 with good periodic autocorrelation. (a) shows the entries of the resultant sequence (i.e. the sequence provided by ITROX when stopped) along with the corresponding binary sequence (obtained by clipping the resultant sequence). The autocorrelation of the binary sequence is shown in (b).



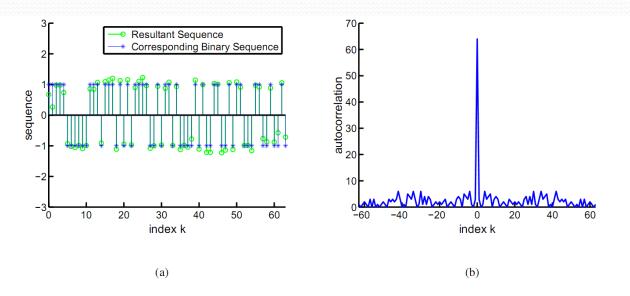
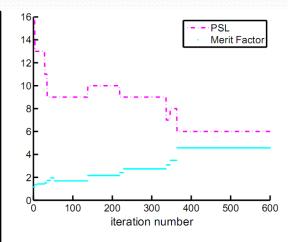


Fig. Design of a binary sequence (of length 64) with good aperiodic autocorrelation. (a) depicts the entries of the resultant sequence (i.e. the sequence provided by ITROX when stopped) along with the corresponding binary sequence (obtained by clipping the resultant sequence). The autocorrelation of the obtained binary sequence is shown in (b).



The binary sequence achieves a PSL value of 6 and a MF of 4.67.



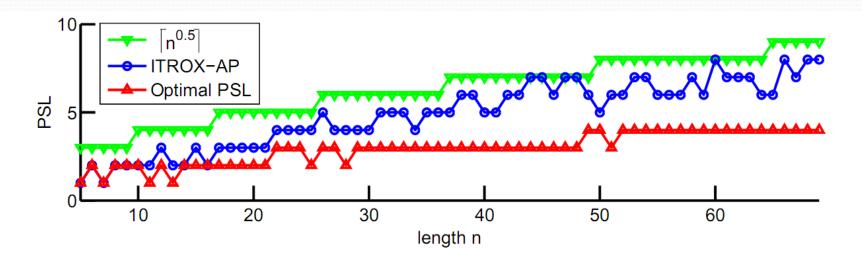


Fig. Comparison of the PSL values of binary sequences generated by ITROX- \mathcal{AP} with the optimal values of PSL and the square root of lengths for $5 \le n \le 69$. For each length, ITROX- \mathcal{AP} was used 5 times and from the 5 resultant PSL values, the best one is shown.



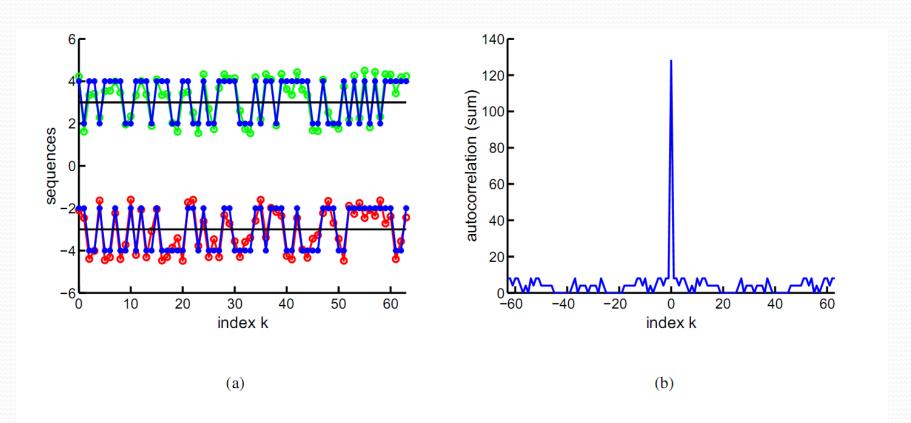


Fig. Design of a binary periodically complementary pair of sequences (both of length 64). (a) plots of the resultant sequences (i.e the sequences provided by ITROX when stopped) along with their corresponding binary sequences (obtained by clipping). A bias of +3 and -3 is used to distinguish the sequences. (b) plot of the autocorrelation sum.



Questions?