Interleaver mapping as Homomorphism: Consider the binary group composed of the set of all the possible \(2^N\) input sequences (\(N\) is the block length). Note that if two input sequences are added, then the terminating phase corresponding to their sum is obtained by adding the terminating phases of the two sequences. This means that the set of the sequences resulting in a zero terminating phase form a sub-group of cardinality \(2^{N-r}\) (called the zero-phase sub-group and denoted by \(P_0\)). This can be considered as the Kernel of the transformation mapping the sequences into their terminating phase. The cosets of this sub-group correspond to the sequences resulting in a given phase other than zero. The number of such cosets is equal to \(K = 2^N - 1\) and each of them contains \(2^{N-r}\) sequences (all with the same terminating phase).

Noting that the interleaving is a linear operation (corresponding to a permutation matrix), we conclude that the interleaver provides a homomorphism with respect to the addition of phases which tries to map the elements of the zero-phase subgroup into its cosets (breaking of the zero-phase sequences). However, as we will see in the following, it is not possible to break all the zero-phase sequences.

Theorem: There does not exist an interleaver which can break all the input sequences with a zero terminating phase.

Proof: Consider two sequences \(A, B\) belonging to the zero-phase subgroup, i.e. \(A, B \in P_0\). Obviously, \(A + B \in P_0\). Assume that the images of \(A\) and \(B\) under the interleaver mapping are equal to, \(I(A)\) and \(I(B)\), respectively. Considering the linearity of the interleaver mapping, we have \(I(A + B) = I(A) + I(B)\). If \(I(A)\) and \(I(B)\) belong to the same coset of \(P_0\) (i.e. have the same terminating phase), then \(I(A + B) \in P_0\) (note that the order of each coset is equal to two). Noting that \(I(A + B) = I(A) + I(B)\), we conclude that \(I(A + B) \in P_0\). Noting that \(A + B \in P_0\), we conclude that the interleaver is not able to break the zero-phase sequence corresponding to \(A + B\). This means that to break the zero phase sequences, they should be mapped to different phases. However, this is not possible because the number of available phases is \(K = 2^N - 1\), while the number of zero-phase sequences is \(2^{N-r}\), which is greater than \(K\) for all the cases of interest.

The best that an interleaver can do in terms of reducing the number of zero-phase sequences, is to distribute the elements of \(P_0\) uniformly among the available phases. In this case, the subset of the zero-phase sequences which remain zero-phase after interleaving is a sub-group of cardinality \(2^{N-r}\) within the zero-phase subgroup. We refer to this sub-group as \(P_0\). The cosets of \(P_0\) are distinguished by a two-tuple coset leader where the first component corresponding to the original phase and the second component corresponds to the phase after interleaving. The number of such cosets is equal to \(2^{N-r}\) and each coset contains \(2^{N-r}\) elements. Similarly, if we use a second interleaver, the best that it can do is to uniformly distribute the elements of \(P_0\) among the available phases. This results in a sub-group \(P_0\) of cardinality \(2^{N-2r}\), which remains zero-phase after breaking of the zero-phase sequences. Continuing in this way, we obtain a nested partition chain of sub-groups where the cosets in the \(k\)th stage are specified by a \(k\)-tuple coset leader. To break all the zero-phase sequences, we should have \(2^{N-r}\) = 1, resulting in a single element (corresponding to the original all zero sequence) for the cosets at the last stage of the interleaving. This requires a value of \(k = N\). Unfortunately, this is impractical for the values of \(N\) and \(K\) which are of interest in practice.

We notice that the best that a single interleaver can do is to reduce the number of the zero-phase sequences from \(2^{N-r}\) to \(2^{N-2r}\). Since in practice \(N > r\), the value of \(2^{N-2r}\) is still a very large number. The conclusion is that the main role of the interleaver is not to break the zero phase sequences, but to (i) provide a large span for the input sequences which have resulted in a zero terminating phase in all the component codes, and (ii) provide a large distance for the terminating edge of the sequences from the right edge of the corresponding block in at least one of the encoders.

Acknowledgements: This work has been supported by the Information Technology Research Centre of Ontario (ITRC).
The simplest case where \( q_k \) consists of a block of contiguous carriers (i.e., \( q_k = (j + (k-1)N/V) j = 1, ..., V \)), which is especially suitable for differential detection systems [1]. Blocks may contain non-contiguous carriers for better PF reduction capability at the cost of extra complexity [3]. Let \( \phi_k, k = 1, ..., N \), be a set of phases with \( \phi_0 = 0 \). The modified symbols \( \tilde{c}_j = c_j e^{j\phi_k(j)} \) for \( j = 1, ..., N \), and \( \tilde{c} = [\tilde{c}_1, \tilde{c}_2, ..., \tilde{c}_N] \). For a given information vector \( c \), the reported optimisation criterion is [1]

\[
[\phi_1, \phi_2, ..., \phi_N] = \arg \min_{[\phi_1, \phi_2, ..., \phi_N]} \|A\|_\infty \tag{4}
\]

Then, the actual transmitted sequence is given by eqn. 3 with this set of block phase factors (\( c \) replaced by \( \tilde{c} \)), which may have to be transmitted by some means (e.g. on extra carriers). To reduce the search complexity, each \( \phi_k \) is discrete and takes a value from the set \( \phi_k \in \{0, \pi/2, \pi, 3\pi/2\} \).

Fig. 1 shows the distribution of the PF for the uncoded case (i.e. there is no attempt to reduce the peak factor) and for a PTS with four blocks. Several observations can be made:

(i) For the uncoded case, the LPF follows the Rayleigh distribution. However, the TPF is \(-0.5\) dB worse than that predicted by the Rayleigh distribution.

(ii) The use of the TPF results in an estimated PF reduction of only \(1\) dB in this case.

(iii) The use of the LPF results in an estimated PF reduction of \(-3\) dB (Fig. 1). The reason seems to be the following: since eqn. 4 is equivalent to suppressing \( |s(t)| \) to move away from the sampling points.

\[ \text{TPF: true peak factor} \quad \text{LPF: lower peak factor} \quad \text{UNC: uncoded} \]

In fact, eqn. 4 is not the only possible optimisation criterion. A recent letter [4] shows that a bound on the PF can be obtained by the sum of the autocorrelation (aperiodic) sidelobe magnitudes of the modulation symbol sequence. This suggests another optimisation criterion. Let \( \rho(k) \) be the aperiodic autocorrelation of \( \tilde{c} \). Then, for a given information vector \( c \), the new optimisation criterion is

\[
[\phi_1, \phi_2, ..., \phi_N] = \arg \min_{[\phi_1, \phi_2, ..., \phi_N]} \sum_{k=1}^{N-1} |\rho(k)| \tag{5}
\]

Fig. 2 shows the PF distribution with the use of eqn. 5. A PF reduction of \(-2.5\) dB can be achieved at \( P_T(\gamma > \alpha) = 10^{-5} \). Note that the difference between the TPF and the LPF is \(-0.5\) dB in this case (Fig. 2). Since the sum in eqn. 5 determines a bound on the true peak, its minimisation leads to a flatter \( |s(t)| \) for \( 0 < t < \tau \), not just on the sampling points. In a practical system, implementing eqn. 5 can be too complicated. For QPSK, the real and imaginary part of each \( p(k) \) can be obtained without any multiplications (the number of integer additions is in the order of \( N^2 \)). So the total complexity varies as \( O(N^{4/3}) \).

Security of the Cao-Li public key cryptosystem

Lim Lek Heng

The author shows that the Cao-Li public key cryptosystem proposed in [1] is not secure. Its private key can be reconstructed from its public key using elementary means such as LU-decomposition and the Euclidean algorithm.

\[ \text{TPF: true peak factor} \quad \text{LPF: lower peak factor} \quad \text{UNC: uncoded} \]

Conclusions: The PTS approach requires that we determine several block phase factors, for which a new optimisation criterion has been presented. Assuming an ideal anti-aliasing filter, the output signal closely resembles the multicarrier signal (eqn. 1). Therefore, it is not sufficient to find the PF on the basis of \( N \) samples. The reported gains of PTS with eqn. 4 appear to be optimistic, however, it may be that the use of a raised-cosine filter alleviates this problem.

\[ \text{TPF for PTS} \quad \text{LPF for PTS} \quad \text{TPF for UNC} \]

References


