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 subgroup correspond to the sequences resulting in a given phase other than zero. The number of such cosets is equal to $K = 2^r - 1$ 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 $I(A) + I(B) \in P_0$ (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 $K = 2^r - 1$, 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-2r} within the zero-phase sub-group. We refer to this sub-group as P_{00}. The cosets of P_{00} are distinguished by a two-tuple coset leader where the first component of the coset-leader corresponds to the original phase and the second component corresponds to the phase after interleaving. The number of such cosets is equal to $2^{2r} - 1$ and each coset contains 2^{N-2r} elements. Similarly, if we use a second interleaver, the best that it can do is to uniformly distribute the elements of P_{00} among the available phases. This results in a sub-group P_{000} of cardinality 2^{N-3r}, which remains zero-phase at all stages of encoding. Continuing in this way, we obtain a nested partition chain of sub-groups where the cosets in the kth stage are specified by a k-tuple coset leader. To break all the zero-phase sequences, we should have $2^{N-kr} = 1$, 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 $k = N/r$. Unfortunately, this is impractical for the values of N and K which are of interest in practice.

We notice that the best 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 $N \gg r$, 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 beak 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.

Acknowledgments: This work has been supported by the Information Technology Research Centre of Ontario (ITRC).

20 August 1997
Electronics Letters Online No: 19980020

A.K. Khandani (*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*)

References

1 BERROU, C., GLAVIEUX, A., and THITIMAJSHIMA, P.: 'Near Shannon limit error-correcting coding and decoding: turbo-codes'. Proc. IEEE Int. Conf. on Comm. 1993 (ICC'93), May 1993, Geneva, pp. 1064–1070
2 GOLOMB, S.W.: 'Shift register sequences' (Holden-Day, San Francisco, 1967)
3 DIVSALAR, D., and POLLARA, F.: 'On the design of turbo codes'. JPL TDA Progress Report 42–123, November 15, 1995
4 BENEDETTO, S., and MONTORSI, G.: 'Design of parallel concatenated convolutional codes', *IEEE Trans. Commun.*, 1996, **44**, pp. 591–600
5 PEREZ, L.C., SEGHERS, J., and COSTELLO, D.J., Jr.: 'A distance spectrum interpretation of turbo codes', *IEEE Trans. Inf. Theory*, 1996, **42**, pp. 1698–1709

Phase optimisation criterion for reducing peak-to-average power ratio in OFDM

C. Tellambura

Recent research suggests combining partial transmit sequences (PTSs) to reduce the peak-to-average power ratio of orthogonal frequency division multiplexing (OFDM). The author presents a new optimisation criterion for PTS and estimates the resulting peak factor reduction.

Introduction: Multicarrier modulation (MCM) is an emerging solution for digital TV broadcasting and wireless communications. In MCM, the signal power can peak to N times the average (for N carriers). Linear amplifiers that can handle the peak power are less efficient. Hard limiting of the signal to reduce the peak power causes performance degradation and spectral sidelobe growth. Thus, partial transmit sequence (PTS) solutions have been investigated [1 – 3]. PTS involves forming several blocks of carriers and multiplying each by a common phase factor. The phase factors are optimised to minimise the peak signal power. In this Letter, a new optimisation criterion and its comparative performance are presented. Also, it is shown that the use of discrete signal samples to estimate the peak level can lead to optimistic estimates of the achievable peak factor reduction.

The signal consists of N complex carriers and hence

$$s(t) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} c_n e^{i[n\Delta\omega t]} \tag{1}$$

where $i = \sqrt{-1}$ and $c_n = e^{i\theta_n}$ ($\theta_n \in \{2\pi k/M \mid k = 0, ..., M-1\}$ is the M-ary phase shift-keying modulation symbol for the nth carrier. If $s(t)$ is sampled at a frequency of $1/T$, the OFDM symbol duration is $\tau = NT$ (for orthogonality $\Delta\omega = 2\pi/NT$). In practice, samples of eqn. 1 are generated by means of an inverse fast Fourier transform (IFFT), and are fed to a digital-to-analogue converter followed by an anti-aliasing lowpass filter. The peak factor (PF) relating to eqn. 1 is defined as

$$\gamma = \max_{0 \leq t < \tau} |s(t)|^2 \tag{2}$$

An N-point IFFT on $\underline{c} = [c_0, ..., c_{N-1}]$ only gives samples of $s(t)$ at time instants $t = kT$ for $k = 0, 1, ..., N-1$. Clearly, the peak amplitude of the IFFT of $\underline{c}$ does not necessarily yield the PF. Therefore, if N samples are used to estimate the PF, this estimate is called the LPF. To get a better estimate, $s(t)$ can be oversampled by a factor of eight, and this estimate is called the TPF. Since LPF $\leq$ TPF $\leq \gamma$, the use of the LPF to estimate the PF reduction of a PTS scheme is prone to error.

PTS optimisation: The IFFT output can be represented by a matrix multiplication as

$$\underline{x} = A\underline{c} \tag{3}$$

where $A = 1/\sqrt{N}[\exp i(2\pi lm/N)]$ $(0 \leq l, m < N)$ is the usual Fourier matrix and $\underline{c}$ is the MPSK symbol sequence. It can be seen that ideal lowpass filtering of $\underline{x}$ gives the waveform in eqn. 1. The PTS approach [2] can be summarised as follows. Divide the symbols c_j between V blocks of N/V symbols. Let $q_k = \{j \mid c_j \in \text{block } k\}$ for $k = 1, ..., V$. The carriers are numbered from 1 to N, and $\cup q_k = \{1,$

..., $N\}$. The simplest case where q_k consists of a block of contiguous carriers (i.e., $q_k = \{j + (k-1)N/V \mid j = 1, ..., N/V \in\}$), 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 ϕ_k, $k = 1, ..., V$, be a set of phases with $\phi_1 = 0$. The modified symbols $\tilde{c}_j = c_j e^{i\phi_k}$ for $j \in q_k$ and $\underline{\tilde{c}} = [\tilde{c}_1, \tilde{c}_2, ..., \tilde{c}_n]$. For a given information vector $\underline{c}$, the reported optimisation criterion is [1]

$$\left[\hat{\phi}_2, \hat{\phi}_3, ..., \hat{\phi}_V\right] = \underset{[\phi_2, \phi_3, \ldots, \phi_V]}{\operatorname{argmin}} \|A\underline{\tilde{c}}\|_\infty \qquad (4)$$

Then, the actual transmitted sequence is given by eqn. 3 with this set of block phase factors ($\underline{c}$ replaced by $\underline{\tilde{c}}$), which may have to be transmitted by some means (e.g. on extra carriers). To reduce the search complexity, each ϕ_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 ~0.5dB worse than that predicted by the Rayleigh distribution.

(ii) The use of the TPF results in an estimated PF reduction of only 1dB for the PTS scheme.

(iii) The use of the LPF results in an estimated PF reduction of 4dB for the PTS scheme.

Therefore, at least in this case, the PTS gains reported [1] appear to be optimistic. Note that the difference between the TPF and the LPF is ~3dB (Fig. 1). The reason seems to be the following: since eqn. 4 is equivalent to suppressing $|s(kT)|$ for $k = 0, ..., N-1$ while keeping the area under $|s(t)|^2$ constant, this very fact *causes* the true peak of $|s(t)|$ to move away from the sampling points.

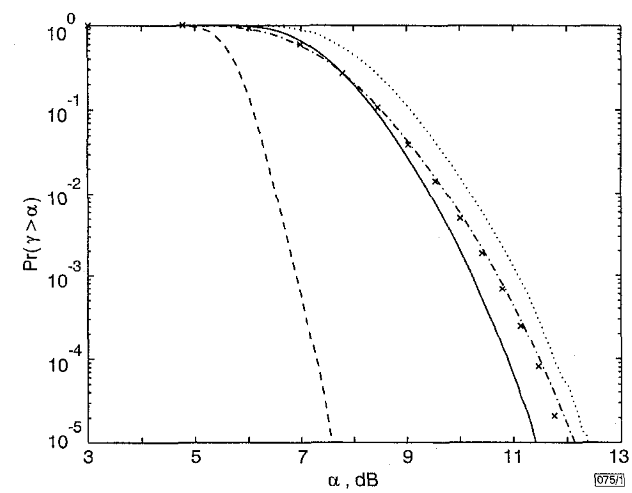

Fig. 1 *Probability that peak factor γ exceeds α for 128 QPSK-modulated carriers*

TPF: true peak factor LPF: lower peak factor UNC: uncoded
Optimisation criterion eqn. 4, 10^6 simulation points
——— TPF for PTS
· — · — · Rayleigh
– – – – LPF for PTS
· · · · · · TPF for UNC
××× LPF for UNC

In fact, eqn. 4 is not the only possible optimisation criterion. A recent Letter [4] shows that a bound on the PF can 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 $\underline{\tilde{c}}$. Then, for a given information vector $\underline{c}$, the new optimisation criterion is

$$\left[\hat{\phi}_2, \hat{\phi}_3, ..., \hat{\phi}_V\right] = \underset{[\phi_2, \phi_3, \ldots, \phi_V]}{\operatorname{argmin}} \sum_{k=1}^{N-1} |\rho(k)| \qquad (5)$$

Fig. 2 shows the PF distribution with the use of eqn. 5. A PF reduction of ~2.5dB can be achieved at $\Pr(\gamma > \alpha) = 10^{-5}$. Note that the difference between the TPF and the LPF is 0.5dB 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 $0 \le t < \tau$, 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 $\rho(k)$ can be obtained without any multiplications (the number of integer additions is in the order of N^2). So the total complexity varies as $O(4^{V-1}N^2)$.

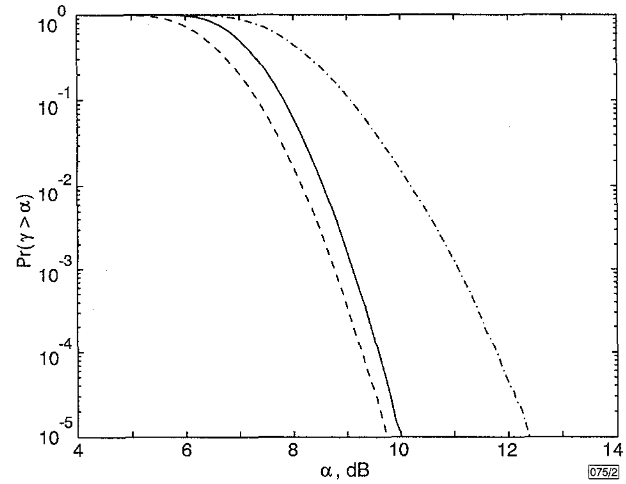

Fig. 2 *Probability that peak factor γ exceeds α for 128 QPSK-modulated carriers*

Optimisation criterion eqn. 5, 10^6 simulation points
——— TPF for PTS
– – – – LPF for PTS
· — · — · TPF for UNC

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.

21 october 1997
Electronics Letters Online No: 19980163

C. Tellambura (*Department of Digital Systems, Monash University, Wellington Road, Clayton, Victoria 3168, Australia*)

E-mail: chintha@dgs.monash.edu.au

References

1 MÜLLER, S.H., and HUBER, J.B.: 'OFDM with reduced peak-to-average power ratio by optimum combination of partial transmit sequences', *Electron. Lett.*, 1997, **33**, pp. 368–369

2 MÜLLER, S.H., BÄUML, R.W., FISCHER, R.F.H., and HUBER, J.B.: 'OFDM with reduced peak-to-average power ratio by multiple signal representation', *Annals of Telecommun.*, 1997, **52**, pp. 58–67

3 MÜLLER, S.H., and HUBER, J.B.: 'A novel peak power reduction scheme for OFDM'. 1997 Int. Sym. on Personal, Indoor and Mobile radio comms. Proc., 1997, (IEEE), pp. 1090–1094

4 TELLAMBURA, C.: 'Upper bound on the peak factor of N-multiple carriers', *Electron. Lett.*, 1997, **33**, pp. 1608–1609

Security of the Cao-Li public key cryptosystem

Lim Lek Heng

The author shows that the Cao-Li 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.

Description of cryptosystem: The Cao-Li public key cryptosystem was first proposed in [1]. It encrypts messages using a bilinear form that is chosen to permit easy decryption by the Chinese remainder theorem. Public key cryptosystems that are designed