using the level six model of a 1µm CMOS technology, and taking for each gate output $C_{LOAD} = 0.1$pF. From Table 1 the following results can be summarised: the PDP of the QAT-HA is one order of magnitude worse than the PDP of the adiabatic binary HA owing to the non fully adiabatic switching, but it is two orders of magnitude better than the PDP of conventional binary and ternary CMOS HA. The saving of area of the QAT-HA in front of the fully adiabatic but binary HA is 65%.

Conclusions: A new low-power logic has been presented. It links adiabatic techniques with the idea of multi-valuation, diminishing the area needed with respect to other adiabatic binary logics and keeping a satisfactory power saving.

© IEE 1996 *12 October 1995*
Electronics Letters Online No: 19960082

D. Mateo and A. Rubio (*Electronic Engineering Department, Universitat Politècnica de Catalunya, Mòdul C4 Campus Nord, C. Gran Capità s/n, 08034 Barcelona, Spain*)

References

1 ATHAS, W.C., SVENSSON, L.'J'., KOLLER, J.G., TZARTZANIS, N., and CHOU, E.Y.: 'Low-power digital systems based on adiabatic-switching principles', *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, 1994, **2**, (4), pp. 398–407

2 HURST, S.L.: 'Multiple-valued logic - its status and its future', *IEEE Trans.*, 1984, **C-33**, (12), pp. 1160–1179

3 YOELI, M., and ROSENFELD, G.: 'Logic design of ternary switching circuits', *IEEE Trans.*, 1965, **EC-14**, pp. 19–29

4 WANG, J.S., WU, C.Y., and TSAI, M.K.: 'Low power dynamic ternary logic', *IEE Proc. G, Electron. Circuits Syst.*, 1988, **135**, (6), pp. 221–230

5 YOUNIS, S.G., and KNIGHT, T.F.: 'Practical implementation of charge recovery asymptotically zero power CMOS'. Proc. 1993 Symp. Integr. Syst., M.I.T. Press, 1993, pp. 234–250

6 YOUNIS, S.G., and KNIGHT, T.F.: 'Asymptotically zero energy split-level charge recovery logic'. Proc. Int. Workshop Low Power Design, Napa, 1994, pp. 177–182

Efficient demodulator for bandpass sampled AM signals

K.G. Larkin

Indexing terms: Signal detection, Nonlinear filters

A simple nonlinear (quadratic) filter is shown to demodulate bandpass sampled AM signals efficiently. The filter is based upon a discrete version of the recently introduced Teager-Kaiser energy operator, but also closely resembles a complex digital sampling demodulator. Such a filter can also be implemented in analogue circuitry.

Introduction: Envelope detectors used for signals, such as AM radio, usually consist of a bandpass filter followed by a nonlinear element (i.e. a square law detector or rectifier) which is, in turn, followed by a low pass filter. Implementation of such a scheme in a digital system is straightforward but inefficient in computational terms because components such as the low pass filter require IIR or FIR digital filters with a considerable number of terms. A more effective alternative such as the complex digital sampling demodulator has a disadvantage owing to oversampling [1]. Recently a nonlinear filter has been developed specifically for AM and FM demodulation of sampled speech signals [2]. A similar nonlinear filter was independently developed for envelope detection in white light interferograms [3]. The technique, however, is applicable to any envelope detection analysis; analogue or digital. The mathematical derivation and analysis of the filter has been detailed in a number of papers [4, 5]. Curiously this analysis assumes that the minimum sampling frequency is about four times the carrier frequency even though careful inspection of the defining equations reveals that apparent 'undersampling' by odd integer factors is also possible as long as the bandpass sampling criterion is satisfied (strictly the Nyquist sampling rate is determined by the bandwidth, but is often used with reference to the maximum frequency). When an already compact and efficient filter is operated in such an undersampling mode the overall efficacy is enhanced greatly. This Letter specifically refers to AM demodulation although a similar analysis can be applied to bandpass sampling FM demodulation.

Nonlinear envelope detector: Consider a narrowband signal $s(t)$ with a DC offset

$$s(t) = a(t) + b(t)\cos(2\pi f_c t + \theta) \qquad (1)$$

where $a(t)$ is the (slowly varying) signal offset, $b(t)$ is the envelope, f_c is the carrier frequency, and θ is the phase offset. It can be shown that the envelope of this signal can be determined from a minimum of four equispaced samples (with unknown spacing) of the signal as long as $a(t)$ and $b(t)$ are sufficiently slowly varying with respect to the period of the carrier [6]. However, using five samples the solution can have a particularly simple form whilst the (bandwidth) constraints upon both $a(t)$ and $b(t)$ can be relaxed considerably. If the separation between samples is τ such that $\Delta = 2\pi f_c\tau$ then

$$4b^2(t)\sin^4(\Delta) = \{s(t+\tau) - s(t-\tau)\}^2 - \{s(t+2\tau) - s(t)\}\{s(t) - s(t-2\tau)\} (2)$$

and

$$\sin^4(\Delta) = 1 \quad \Rightarrow \quad \Delta = (2n+1)\frac{\pi}{2} \qquad (3)$$

The undersampling factor in the above equation is $(2n+1)$ where n is an positive integer. Hence if τ is chosen to be approximately one quarter of the carrier period or any odd multiple thereof, then the gain factor $\sin^4(\Delta)$ will be near unity. Eqn. 2 indicates that the envelope squared can be computed from just five samples using a difference operation followed by two multiplications. Computationally this represents a compact and efficient digital demodulator. Fig. 1 shows the circuit equivalent of eqn. 2, which may be implemented as an analogue or a digital system.

Operation of the filter: The 3dB gain bandwidth of the filter is controlled by the value of $\sin^4\Delta$ in eqn. 2:

$$(n + 0.32)\pi \leq \Delta \leq (n + 0.68)\pi \qquad (4)$$

In the full sampling case $n = 0$, and the nominal sampling frequency is four times the carrier frequency. Eqn. 4 then shows well over an octave of useable gain bandwidth for the squared envelope process.

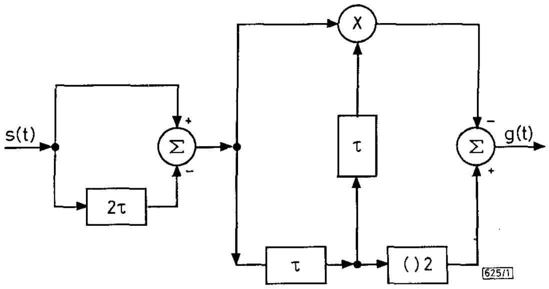

Fig. 1 *Schematic diagram of sampling demodulator based on second order nonlinear filter*

Circuit may be digital or analogue

The operational principle of the overall system can be described rather simply. The linear difference acts as a simple bandpass filter with a peak at one quarter of the sample frequency. It is essential that any unwanted sidebands, including DC, be removed before quadratic filtering. Quadratic filters are known to produce zero (baseband) and second harmonic signals from monochromatic input [6, 7]. Both the squared term and the cross product term of eqn. 2 produce baseband and second harmonic terms. The relative phase shifts of both cross-product components combine to produce a second harmonic exactly in antiphase to that of the squared term. Such a neat cancellation does not occur at baseband so the end result is a square-law envelope detector which removes its own second harmonics by phased cancellation rather than by fixed frequency low pass filtering.

An alternative explanation of the operational principle is that the system is a quadrature receiver (see e.g. Whalen [9]) which derives the quadrature signal from the input signal rather than from a local oscillator. A third explanation of the filter in terms of signal 'energy' and its relation to first and second derivatives of the signal has been particularly fruitful for the development of rigorous bounds on performance in relation to noise and bandwidth parameters [3].

Performance of the undersampling envelope detector: Undersampling has a simple effect: the bandwidth limits determined by Maragos et al [4] merely have to be reduced in proportion to the undersampling factor ($2n$+1). So, for example, undersamplIng by a factor of 3 reduces the predicted maximum modulation bandwidth by a factor of 3. The bandwidth restrictions have been based on the signal to error ratio (SER). The error being the difference between an ideal demodulated signal and the signal demodulated by the actual filter defined by eqn. 2. Once a minimum SER has been defined then the maximum modulation bandwidth can be calculated from formulas given in [3]. The usual bandpass sampling requirements still apply [9], i.e. if B is the bandwidth then

$$B(2n+1) \leq f_c \qquad (5)$$

In the schematic diagram of the quadratic filter demodulator shown in Fig. 1 the sampling frequency is simply controlled by the delay τ. To demonstrate the principle of undersampling, the outputs of such a demodulator (after performing a square root operation) have been simulated for two sampling cases. The chosen input has a Gaussian envelope and the bandwidth is about one tenth of the carrier frequency. The envelope derived by full sampling demodulation is shown in Fig. 2*a*. The corresponding plot for three times undersampling is shown in figure Fig. 2*b*. Clearly the signal to error ratio has deteriorated because the modulation bandwidth was not reduced by the requisite factor of 3. Fig. 2*c* shows the difference between *a* and *b* magnified by a factor of 10 for clarity. An extreme modulation bandwidth has been used to accentuate the errors. In practice, bandwidths of < 1% of the carrier frequency are typical. As the SER is proportional to the square of {sampling frequency/modulation bandwidth} typical errors can be expected to be at least 20dB lower than shown.

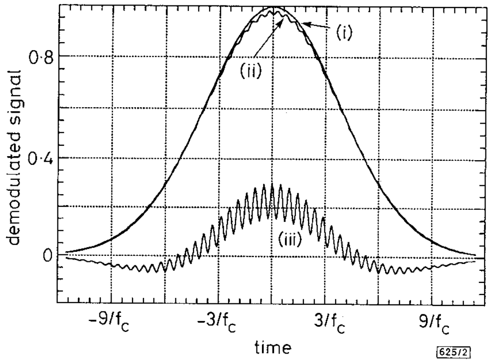

Fig. 2 *Demodulated envelopes from AM signal (DSBSC) with large bandwidth Gaussian envelope*

(i) Envelope produced by nonlinear filter with full sampling, namely 4 times carrier frequency
(ii) Envelope produced by 3 times undersampling
(iii) 10 × difference between *a* and *b*

Conclusion: A remarkably efficient nonlinear filter has been shown to work with an undersampled signal, further reducing the computational load. A direct trade-off between demodulation errors and undersampling ratio applies for signals with a given bandwidth. In situations where computational effiency is paramount such a filter may be invaluable.

Acknowledgments: It is a pleasure to express my gratitude to C. Sheppard for his assistance and encouragement during the the preparation of this Letter, which constitutes part of my doctoral research programme.

© IEE 1996 *23 August 1995*
Electronics Letters Online No: 19960081

K.G. Larkin (*Department of Physical Optics, School of Physics, The University of Sydney, NSW 2006, Australia*)

References

1 THIEL, T.E., and SAULNIER, G.J.: 'Simplified complex digital sampling demodulator', *Electron. Lett.*, 1990, **26**, (7), pp. 419–421

2 KAISER, J.F.: 'On a simple algorithm to calculate the 'energy' of a signal'. Proc. IEEE Int. Conf. Acoust. Speech, Signal Process., Albuquerque, NM, 1990, pp. 381–384

3 LARKIN, K.G.: 'Neat nonlinear algorithm for envelope detection in white light inferometry', submitted to *J. Opt. Soc. Am. A, Opt. Image Sci.*, 1995

4 MARAGOS, P., KAISER, J.F., and QUATIERI, T.F.: 'On amplitude and frequency demodulation using energy operators', *IEEE Trans. Signal Process.*, 1993, **42**, (4), pp. 1532–1550

5 BOVIK, A.C., and MARAGOS, P.: 'Conditions for positivity of an energy operator', *IEEE Trans. Signal Process.*, 1994, **41**, (2), pp. 469–471

6 CARRE, P.: 'Installation et utilisation du comparateur photoelectrique et interferentiel du Bureau International des Poids et Mesures', *Metrologia*, 1966, **2**, (1), pp. 13–23

7 PICINBONO, B.: 'Quadratic filters'. Proc. IEEE Int. Conf. Acoust. Speech, Signal Process., 1982, pp. 298–301

8 PITAS, I., and VENETSANOPOULOS, A.N.: 'Nonlinear digital filters: Principles and applications' (Kluwer Academic Publishers, Boston, 1990)

9 WHALEN, A.D.: 'Detection of signals in noise' (Academic Press, New York, 1971)

10 VAUGHAN, R.G., SCOTT, N.L., and WHITE, D.R.: 'The theory of bandpass sampling', *IEEE Trans. Signal Process.*, 1991, **39**, (9), pp. 1973–1984

Note on decoding binary Goppa codes

K. Huber

Indexing terms: Codes, Error correction codes, Decoding

The author gives a simple expression for the polynomial $y(x)$ which solves the polynomial equation $y(x)^2 \equiv t(x) \bmod G(x)$, where $t(x)$, $y(x)$ and $G(x)$ are polynomials over the field $GF(2^m)$. The solution of such an equation is a step in the so called Patterson algorithm for decoding binary Goppa codes. The result may also be useful for other applications.

Introduction: For theoretical as well as practical purposes Goppa codes [3 – 5] are among the most interesting and fascinating classes of block codes. A further important application of Goppa codes stems from the introduction of the public key cryptosystem of McEliece [6]. Goppa codes can be decoded in an elegant algebraic way by using the extended Euclidean or the Berlekamp-Massey algorithm [8, 4, 5]. The Patterson algorithm for decoding binary Goppa codes ([8], algorithm 4) needs the solution of a polynomial equation of the following kind as a second step:

$$y(x)^2 \equiv t(x) \bmod G(x) \qquad (1)$$

i.e. we are given the polynomials $t(x)$ and $G(x)$ over the field $GF(2^m)$ and want to determine the polynomial $y(x)$. In fields of characteristic two the operation of taking square roots is a linear operation, hence the usual way of taking the square root of $t(x)$ mod $G(x)$ is to perform this linear operation using a matrix (see e.g. [8, 2] section 2.44). In the following we show that the solution of eqn. 1 can be expressed in a very simple closed form, which is very useful for direct implementation in software or hardware.

Taking square roots of polynomials modulo $G(x)$: First we set $G(x) = g_1(x)^2 + x \cdot g_2(x)^2$, hence

$$g_1(x)^2 \equiv x \cdot g_2(x)^2 \bmod G(x)$$

Assuming that $G(x) = G_0 + G_1x + \ldots G_sx^s$ with $G_0 \neq 0$, we know that the greatest common divisor (gcd) of x and $G(x)$ equals 1, hence there is a polynomial $w(x)$ such that $w(x)^2 \equiv x \bmod G(x)$.