stage of power supplies in most equipment. Fig. 3 shows the corresponding waveforms with the active filter connected to the circuit. This was achieved by optimising for 41 harmonics.

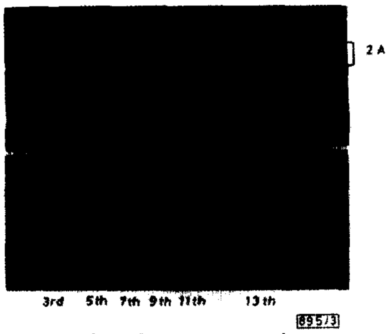

Fig. 3 *Current waveform after compression and its spectrum*

Conclusion: This novel approach for the design of active filters provides an alternative method of controlling current harmonics generated by nonlinear loads such as rectifiers. Whereas a conventional filter circuit can only attenuate a range of harmonics, the proposed approach can achieve almost complete elimination. It would be suitable for applications where the magnitude, phase and range of current harmonics are not predictable. On-line control of the filter would provide a good solution.

10 January 1995
Electronics Letters Online No: 19950750

Z.D. Koozehkanani, P. Mehta and M.K. Darwish (*Bruner University, Department of Electrical Engineering, Uxbridge, Middlesex UB8 3PH, United Kingdom*)

References

1 CHOE, G., and MIN-HO, P.: 'A new injection method for AC harmonics elimination by active power filters'. *IEEE Trans. Ind. Electron.*, 1988, **35**, (1), pp. 141–147
2 MEHTA, P., DARWISH, M., and THOMSON, T.: 'Switched-capacitor filters', *IEEE Trans.*, 1990, **PE-5**, (3), pp. 331–337
3 LUENBERGER, D.G.: 'Linear and non-linear programming' (Addison-Wesley, 1984)

High input impedance filters with low component spread using current-feedback amplifiers

Shen-Iuan Liu

Indexing terms: Current conveyors, Active filters

A new configuration for high input impedance bandpass, lowpass and highpass filters with low component spread using two current-feedback amplifiers is presented. It has the following features: orthogonal control of the natural frequency and quality factor by grounded resistors or capacitors, simple conversion into a voltage-controlled filter, minimum active components, low active and passive sensitivities, low component spread suitable for high-Q applications and low output impedance. Experimental results are given to demonstrate the feasibility of the proposed circuits.

Introduction: Single-amplifier biquads use few components to realise the required filtering functions [1], but large passive and active sensitivities limit their range of applications. Multiple-amplifier biquads can have relaxed passive and active sensitivities with respect to components. High input impedance biquads using a single second-generation current conveyor (CCII) [2] or multiple CCIIs [3, 4] have been developed. Although the high input impedance filters using CCIIs have low sensitivities, they are subject to the large component spread for high-Q applications (i.e. the component spread is proportional to Q^2). Recently, by using current-feedback amplifiers (CFAs) to realise active-RC filters, oscillators and immittance simulating circuits have been receiving significant attention [4 – 8]. In this Letter, a new configuration for high input impedance bandpass, lowpass, and highpass filters with low component spread by using two CFAs is presented. The natural frequency and quality factor of a bandpass filter can be adjusted by grounded resistors.

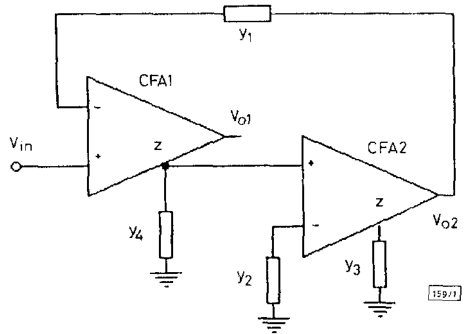

Fig. 1 *Configuration for realising high input impedance filters using two CFAs*

Circuit description: A CFA is equivalent to the combination of a second-generation current conveyor [9] and a voltage buffer [10]. Its port relations can be modelled as $I_+ = 0$, $V_- = V_+$, $I_Z = I_-$ and $V_o = V_Z$. Considering the proposed configuration in Fig. 1, its transfer functions can be expressed as

$$\frac{V_{o1}}{V_{in}} = \frac{y_1 y_3}{y_1 y_2 + y_3 y_4} \tag{1}$$

and

$$\frac{V_{o2}}{V_{in}} = \frac{y_1 y_2}{y_1 y_2 + y_3 y_4} \tag{2}$$

From eqns. 1 and 2, the bandpass, lowpass and highpass filters can be realised as follows. If the admittances are: $y_1 = sC_1$, $y_2 = sC_2 + 1/R_2$, $y_3 = 1/R_3$ and $y_4 = 1/R_4$, a bandpass filter can be obtained at node V_{o1} in Fig. 2 and its transfer function is

$$\frac{V_{o1}}{V_{in}} = \frac{sC_1R_4}{1 + s\frac{C_1R_3R_4}{R_2} + s^2R_3R_4C_1C_2} \tag{3}$$

From eqn. 3, the natural frequency ω_o and quality factor Q of this filter are

$$\omega_o = \frac{1}{\sqrt{R_3R_4C_1C_2}} \qquad Q = \frac{R_2\sqrt{C_2}}{\sqrt{R_3R_4C_1}} \tag{4}$$

Thus, ω_o and Q can be orthogonally adjustable by grounded resistors. Moreover, its component spread can only be proportional to Q and all the resistors of this filter are grounded. When a grounded resistor is replaced by a JFET transistor, a voltage-controlled filter can be obtained.

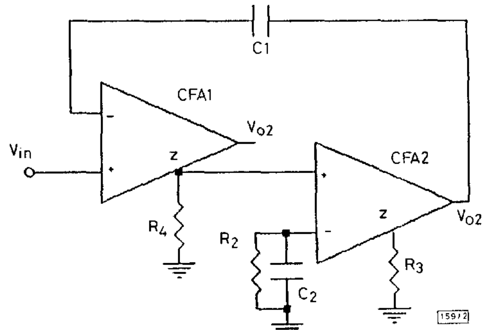

Fig. 2 *High input impedance bandpass filter using two CFAs*

Taking into account the nonideal CFAs, namely $I_Z = \alpha I_x$, $V_x = \beta V_y$ and $V_o = \gamma V_Z$ where $\alpha = 1 - \varepsilon_1$ and ε_1 ($\varepsilon_1 << 1$) denotes the current tracking error of a CFA, $\beta = 1 - \varepsilon_2$ and ε_2 ($\varepsilon_2 << 1$) is the input voltage tracking error, and $\gamma = 1 - \varepsilon_3$ and ε_3 ($\varepsilon_3 << 1$) is the output voltage tracking error. The natural frequency ω_o and quality factor Q can be rewritten as

$$\omega_o = \sqrt{\frac{1}{C_1C_2R_3R_4\alpha_1\alpha_2\beta_2\gamma_2}}$$
$$Q = R_2\sqrt{\frac{C_2}{C_1R_3R_4\alpha_1\alpha_2\beta_2\gamma_2}} \quad (5)$$

The active and passive sensitivities of this bandpass filter are

$$S^{\omega_o}_{\alpha_1,\alpha_2,\beta_2,\gamma_2} = \frac{-1}{2} = S^{\omega_o}_{R_3,R_4,C_1,C_2}$$
$$= S^{Q}_{\alpha_1,\alpha_2,\beta_2,\gamma_2,C_1,C_2,R_3,R_4} = -S^{Q}_{C_2}$$
$$S^{\omega_o}_{\beta_1,\gamma_1} = S^{Q}_{\beta_1,\gamma_1} = 0 \qquad S^{Q}_{R_2} = 1$$

All the active and passive sensitivities are no greater than unity.

Similarly, another high input impedance bandpass filter with all grounded capacitors can be constructed if the admittances are: $y_1 = 1/R_1$, $y_2 = sC_2 + 1/R_2$, $y_3 = sC_3$ and $y_4 = sC_4$. It is attractive to use grounded capacitors in monolithic integration [11]. Its transfer function can be expressed as

$$\frac{V_{o1}}{V_{in}} = \frac{sC_3R_2}{1 + sR_2C_2 + s^2R_1R_2C_3C_4} \quad (6)$$

Its natural frequency ω_o and quality factor Q can be expressed as

$$\omega_o = \frac{1}{\sqrt{R_1R_2C_3C_4}}$$
$$Q = \frac{\sqrt{R_1C_3C_4}}{C_2\sqrt{R_2}}$$

Furthermore, according to eqn. 2, a lowpass filter at node V_{o2} in Fig. 1 can be obtained if the admittances are: $y_1 = 1/R_1$, $y_2 = 1/R_2$, $y_3 = sC_3 + 1/R_3$ and $y_4 = sC_4$. Similarly, a highpass filter can be obtained at node V_{o2} in Fig. 1 if the admittances are : $y_1 = sC_1$, $y_2 = sC_2$, $y_3 = sC_3 + 1/R_3$ and $y_4 = 1/R_4$. The passive and active sensitivities of the four proposed filters are all no greater than one.

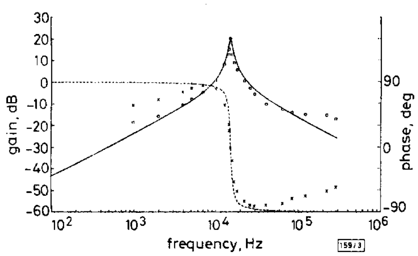

Fig. 3 *Comparisons between theoretical and experimental results for bandpass filter in Fig. 2 with $C_1 = C_2 = 10nF$, $R_3 = R_4 = 1k\Omega$ and $R_2 = 10k\Omega$*

——— gain, theoretical
– – – – phase, theoretical
O gain, experimental
× phase, experimental

Experimental results: To verify the theoretical analysis, the proposed second-order bandpass filter in Fig. 2 is implemented by using commercial CFAs (AD844) [12]. The power supply is ±5V and the component values are: $C_1 = C_2 = 10$nF, $R_3 = R_4 = 1$kΩ and $R_2 = 10$kΩ (i.e. $Q = 10$ and $\omega_o/2\pi = 15.9$kHz). Fig. 3 shows the experimental results for this filter.

Conclusions: New high input impedance bandpass, lowpass, and highpass filters using two CFAs are presented. They provide the following advantages: orthogonal control of their natural frequency and quality factor by grounded resistors or capacitors, ease of conversion into a voltage-controlled filter, minimum active components, low passive and active sensitivities, low component spread for high-Q applications and low output impedance. The proposed circuits are expected to be useful in analogue filtering applications.

1 May 1995
Electronics Letters Online No: 19950725

Shen-Iuan Liu (*Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 10664, Republic of China*)

References

1 SEDRA, A., and BRACKETT, P.O.: 'Filter theory and design: active and passive' (Matrix Publisher, Illinois, 1978)
2 LIU, S.I., and TSAO, H.W.: 'The single CCII biquad with high-input impedance', *IEEE Trans.*, 1991, **CAS-38**, pp. 456–461
3 NAQSHBANDI, S.F.H., and SHARMA, R.S.: 'High input impedance current conveyor filters', *Int. J. Electron.*, 1983, **55**, pp. 499–500
4 FABRE, A., DAYOUB, F., DURUISSEAU, L., and KAMOUN, M.: 'High input impedance insensitive second-order filters implemented from current conveyors', *IEEE Trans.*, 1994, **CASI-41**, pp. 918–921
5 LIU, S.I., and HWANG, Y.S.: 'Realisation of R-L and C-D impedances using a current-feedback amplifier and its applications', *Electron. Lett.*, 1994, **30**, pp. 380–381
6 WU, D.S., HWANG, Y.S., LIU, S.I., and WU, Y.P.: 'New multifunction filter using an inverting CCII and a voltage follower', *Electron. Lett.*, 1994, **30**, pp. 551–552
7 CHANG, C.M., HWANG, C.S., and TU, S.H.: 'Voltage-mode notch, lowpass and bandpass filter using current-feedback amplifiers', *Electron. Lett.*, 1994, **30**, pp. 2022–2023
8 WU, D.S., LIU, S.I., HWANG, Y.S., and WU, Y.P.: 'Multiphase sinusoidal oscillator using the CFOA pole', *IEE Proc. G*, 1995, **142**, pp. 37–40
9 SEDRA, A., and SMITH, K.C.: 'A second generation current conveyor and its applications', *IEEE Trans.*, 1970, **CT-17**, pp. 132–134
10 SVOBODA, J.A., MCGORY, L., and WEBB, S.: 'Applications of a commercially available current conveyor', *Int. J. Electron.*, 1991, pp. 159–164
11 BHUSAN, M., and NEWCOMB, R.W.: 'Grounding of capacitors in integrated circuits', *Electron. Lett.*, 1967, **3**, pp. 148–149
12 Analog devices: 'Linear products data book' (Norwood, MA, 1990)

Key-spoofing attacks on nested signature blocks

B. Christianson and M.R. Low

Indexing terms: Cryptography, Public key cryptography

For a given signature block and any other data, there exists a key which produces the same signature block. The threat that this poses to schemes which use nested signature blocks as pointers to other tokens is identified, using a theft-proof capability mechanism as an illustration. A modification to public key certificates is then proposed to eliminate this threat.

Introduction: It is frequently desirable to include public key signatures within other pieces of text that are themselves signed. For example, public key cryptography [1, 2] allows construction of theft-proof capabilities that can be held in the user space, passed across untrusted networks, and used without on-line authentication of the presenter at the time of access, but that cannot be used by an impostor even temporarily and even with the collusion of public key certification authorities. Associated with each such capability is a signature, which is the result of the granting principal applying their private key to a one-way hash of the capability contents. Using such capabilities efficiently, it is desirable to refer to them by their signatures in other electronically signed instruments such as service requests, rather than including their complete text. There are many other cases (for example in audit trails) where similar signature nesting is desirable. Unfortunately, signature nesting allows a key-spoofing attack [3], because for many public key cryptosystems (including RSA) it is possible for an attacker to find a bogus key under which a bogus message has the same signature as the genuine message under the genuine key. Collusion with a certification authority can now allow short-term use of a (supposedly) theft-proof capability by an impostor. Such an attack can be prevented by forcing nested signatures to include the public key of the signer. In particular, if the signatures of public key certificates are embedded in other signed text such as