MAKHOUL'S CONJECTURE FOR $P = 2$

Nigel Boston

Department of Mathematics and Coordinated Science Laboratory
University of Illinois
Urbana, IL 61801
n-boston@comm.csl.uiuc.edu

ABSTRACT

Last year, the IEEE Signal Processing Society offered a prize of $1000 for proving or disproving Makhoul's conjecture, which says that, given a causal all-pass digital signal x_n of order p, with nonzero x_0, the location of the peak of x_n always lies between $n = 0$ and $n = 2p - 1$. The case of $p = 1$ is trivial, and no further progress had been made in 25 years until Lertniphonphun, Rajagopal, and Wenzel gave counterexamples for large p. In this paper, Makhoul's conjecture is proven for $p = 2$. It is also shown that the conjecture fails dramatically in the case of complex coefficients.

1. The Preliminaries.

If x_n is the impulse response of an all-pass digital filter of order $p = 2$, then x_n satisfies a recurrence relation

$$x_n + bx_{n-1} + ax_{n-2} = a\delta_n + b\delta_{n-1} + \delta_{n-2}$$

with $x_{-2}, x_{-1} = 0$, where a, b are real numbers, $a \neq 0$, such that the roots of $x^2 + bx + a$ (call them α, β) lie strictly inside the unit circle. Thus, e.g. $x_0 = a$, $x_1 = b - ab$, $x_2 = 1 - a^2 - b^2 + ab^2$.

We first obtain a nice representation of x_n.

Lemma. $x_0 = \alpha\beta$; if $n \geq 1$, then

$$x_n = (\alpha\beta - 1)(g_n(\alpha) - g_n(\beta))/(\alpha - \beta) \quad (\alpha \neq \beta),$$

$$x_n = (\alpha^2 - 1)g_n'(\alpha) \quad (\alpha = \beta),$$

where $g_n(x) = x^{n+1} - x^{n-1}$.

Note that because $\alpha\beta$ is never 1, we can equivalently consider the sequence y_n where $y_n = x_n/(\alpha\beta - 1)$. Note $y_0 = \alpha\beta/(\alpha\beta - 1), y_1 = \alpha + \beta, y_2 = \alpha^2 + \alpha\beta + \beta^2 - 1, \ldots$.

This work was supported by NSF DMS 99-70184. The author thanks Andrew Singer for introducing him to the problem.

2. The Repeated Roots Case.

In this case α is real. Since g_n' is either even or odd, we simply need to show that $g_n'(\alpha)$ $(= (n+1)\alpha^n - (n-1)\alpha^{n-2} = y_n)$ is always less than 2α $(= y_1)$ for $\alpha \in (0, 1)$ and $n \geq 2$. (This is actually a limiting case of case I below.) One easily checks that $2x - (n+1)x^n + (n-1)x^{n-2}$ is positive for $x \in (0, 1)$.

3. The Real Roots Case.

Suppose α and β are both real.

Case I. $\alpha, \beta \geq 0$.

Without loss of generality assume $\alpha > \beta$. Let $n \geq 2$. Recall $g_n(x) = x^{n+1} - x^{n-1}$. One easily checks that $x^2 - g_n(x)$ is an increasing function of x in $[0, 1]$. Then $\alpha^2 - g_n(\alpha) > \beta^2 - g_n(\beta)$. So $\alpha^2 - \beta^2 > g_n(\alpha) - g_n(\beta)$, so $\alpha + \beta > y_n$. Likewise, since $x^2 + g_n(x)$ is an increasing function of x in $[0, 1]$, it follows that $\alpha + \beta > -y_n$.

Case II. $\alpha, \beta \leq 0$.

The substitution $\alpha \mapsto -\alpha, \beta \mapsto -\beta$ sends y_n to $(-1)^n y_n$, which does not affect absolute values, and so this case reduces to case I.

Case III. $\alpha \geq 0, \beta \leq 0$.

Let $n \geq 3$. Consider the function $x - x^3 - g_n(x)$. This is positive if $x > 0$ and negative if $x < 0$. Thus, $\alpha - \alpha^3 - g_n(\alpha) > \beta - \beta^3 - g_n(\beta)$, so $\alpha - \alpha^3 - \beta + \beta^3 > g_n(\alpha) - g_n(\beta)$. Dividing by $\alpha - \beta$, we get $-(\alpha^2 + \alpha\beta + \beta^2 - 1) > y_n$. Likewise, using $x - x^3 + g_n(x)$, we get

$-(\alpha^2+\alpha\beta+\beta^2-1) > -y_n.$

To summarize, in each case, we have the absolute value of y_1 or of y_2 exceeding the absolute value of y_n for any $n \geq 3$. This establishes Makhoul's conjecture in this case (in fact something stronger, since y_0 and y_3 are not employed).

4. The Complex Roots Case.

Assume that α and β are complex conjugates. The question of which of $x_0, x_1, ...$ is largest now becomes quite complicated. The proof proceeds in a similar manner to before. We wish to prove inequalities of the form $\mid g_m(\alpha) - g_m(\beta) \mid > \mid g_n(\alpha) - g_n(\beta) \mid$ for various m, n. If we suppose $g_n(x) = h(g_m(x))$ for some function h, then we wish to obtain an upper bound of 1 for $(\mid h(\gamma) - h(\delta) \mid)/(\mid \gamma - \delta \mid)$, where $\gamma = g_m(\alpha)$ and $\delta = g_m(\beta)$. This is achieved by the Intermediate Value Theorem, saying that this equals $h'(c)$ for some c between γ and δ, and then bounding $h'(c)$. Note that $g_n'(x) = h'(g_m(x))g_m'(x)$. If $c = g_m(d)$, then $h'(c) = g_n'(d)/g_m'(d)$.

Let $r = \mid \alpha \mid = \mid \beta \mid$. We combine the above with the observation that if $r \geq \sqrt{2/3}$, then y_0 $(= r^2/(r^2-1))$ has absolute value ≥ 2, whereas clearly y_n $(n \geq 1)$ has absolute value < 2. Thus, it just remains to check cases where $r < \sqrt{2/3} = 0.816....$

The cases $m = 1, 2, 3$ lead to us seeking upper bounds for $(n+1)x^n - (n-1)x^{n-2}$ divided by (respectively) $2x, 3x^2-1, 4x^3-2x$ in the region $\mid x \mid < \sqrt{2/3}$. One can show that these always have absolute value less than 1 if respectively $n \geq 16, 11, 9$. It is interesting that this leaves us now with a finite check and also that x_3 leaves us with the shortest such check. A similar but finer analysis of the cases $4 \leq n \leq 8$ yields that in each case (in the region $\mid x \mid < \sqrt{2/3}$) one of x_1, x_2, x_3 has larger absolute value than x_n.

5. The Complex Coefficients Case.

At the end of his conjecture challenge paper, Makhoul states his belief that the conjecture also holds in the case of complex coefficients. This is false. Consider e.g. $\alpha = \beta = ri$ as r varies from 0 to 1. Then $x_n = (-r^2-1)g_n'(ri)$, which has absolute value $r^{n-2}(r^2+1)((n+1)r^2+(n-1))$. For a given value of r, we consider this as a function of n. Differentiating with respect to n, we see that this function has a maximum at $n = -(1+r^2+(r^2-1)\log r)/((1+r^2)\log r)$, which increases steadily from 1 to infinity as r goes from 0 to 1. The value of the function at this n exceeds 1 and so exceeds $\mid x_0 \mid = r^2$.

In this way, we obtain cases where x_n attains its maximal absolute value for arbitrarily large n. (Of course, we only need one example to show the falsehood of this conjecture.)

6. An Alternative Approach.

The following approach is more systematic, explains the role of $2p-1$, and should generalize to larger p.

Lemma. If $n \geq 5$, then $x_n = F(x_{n-4}, x_{n-3}, x_{n-2}, x_{n-1})$, where F is the function $\mathbf{R^4} \to \mathbf{R}$ defined by

$$F(t,x,y,z) := (y^3 + tz^2 - 2xyz)/(ty - x^2).$$

Proof. Since $x_n + bx_{n-1} + ax_{n-2} = 0$ and $x_{n-1} + bx_{n-2} + ax_{n-3} = 0$ and $x_{n-2} + bx_{n-3} + ax_{n-4} = 0$, we obtain a matrix equation

$$\begin{pmatrix} x_n & x_{n-1} & x_{n-2} \\ x_{n-1} & x_{n-2} & x_{n-3} \\ x_{n-2} & x_{n-3} & x_{n-4} \end{pmatrix} \begin{pmatrix} 1 \\ b \\ a \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Thus, the determinant of the 3-by-3 matrix is 0. Solving for x_n in terms of $x_{n-4}, ..., x_{n-1}$ gives the lemma.

Note that the function F is "universal" for the case $p = 2$ in that it does not involve any particular a and b. Let V denote

$$\{(t,x,y,z) : \mid F(t,x,y,z) \mid < max(\mid t \mid, \mid x \mid, \mid y \mid, \mid z \mid)\}.$$

This is a very interesting subset of $\mathbf{R^4}$. For instance, it has the property that if $\underline{x} \in V$, then $\lambda \underline{x} \in V$ for any $\lambda \in \mathbf{R}^*$. Thus, V can be considered as a subset of projective space $\mathbf{P^3}(\mathbf{R})$, which is compact. It makes sense then to ask what the measure of V is. Computations suggest it is exactly 0.5; in other words, half of the elements of $\mathbf{R^4}$ lie in V.

For our purposes, we are interested in particular elements of $\mathbf{R^4}$, namely those 4-tuples $(x_{n-4}, x_{n-3}, x_{n-2}, x_{n-1})$ arising from second order recurrence relations with real coefficients. Let W be the subset of such 4-tuples (running over all n and all such recurrence relations). The following claim appears to be true but the proof is as yet incomplete. The "right" proof should perhaps come from the field of semialgebraic geometry. Computations confirm the claim.

Claim. $W \subseteq V$.

Consequence. The location of the peak for any all-pass digital signal of order 2 occurs for $n \leq 4$.

Proof. Let $m = max(\mid x_1 \mid, \mid x_2 \mid, \mid x_3 \mid, \mid x_4 \mid)$. The proof establishes by induction on n that $\mid x_n \mid \leq m$ and $< m$ if $n \geq 5$. This is certainly true for $n \leq 4$. Suppose it is true for all $n < N$. Then $x_N = F(x_{N-4}, x_{N-3}, x_{N-2}, x_{N-1})$ and, since by the above claim $(x_{N-4}, x_{N-3}, x_{N-2}, x_{N-1}) \in V$, $\mid x_N \mid < max(\mid x_{N-4} \mid, \mid x_{N-3} \mid, \mid x_{N-2} \mid, \mid x_{N-1} \mid) \leq m$, and we're done.

A little extra work reduces this to $n \leq 3$. Note that for general p, the same method leads to x_n being expressed as a rational function of $x_{n-2p}, ..., x_{n-1}$, and we obtain a set with properties similar to V above.