An Elementary Proof of the Inequality: variance $\leq (M - \overline{x})(\overline{x} - m)$

Vedula N. Murty

Introduction.

Whenever I proved an inequality using calculus my teacher always asked me, "See if you can prove it without using calculus". Bhatia and Davis [1] gave a new bound for the variance, and their proof used calculus. The object of this note is to present an elementary proof of their result without using calculus.

In this paper we assume that $x_1, \ldots, x_n$ are real numbers. Recall that the variance of these numbers is defined to be

$$\sigma^2 = \frac{1}{n}\sum_{j=1}^{n}(x_j - \overline{x})^2, \quad \text{where} \quad \overline{x} = \frac{1}{n}\sum_{j=1}^{n} x_j.$$

Let $M = \max\{x_1, x_2, \ldots, x_n\}$ and $m = \min\{x_1, x_2, \ldots, x_n\}$, and set $R = M - m$. The classical bound on the variance, known to students of statistics, is

$$\sigma^2 \leq \frac{R^2}{4}. \tag{1}$$

In [1] Bhatia and Davis proved

$$\sigma^2 \leq (M - \overline{x})(\overline{x} - m). \tag{2}$$

It is easy to show that the right hand side of (2) is less than or equal to the right hand side of (1) (as we will do following the proof below). This shows that the new bound is sharper than the classical bound.

An Elementary Proof.

Given the population $x_1, x_2, \ldots, x_n$, note that its variance, mean, maximum, and minimum are invariant under a permutation of the x_j's. We, therefore, establish (2) assuming

$$x_1 \leq x_2 \leq \ldots \leq x_n. \tag{3}$$

Now (3) implies $M = x_n$ and $m = x_1$. Thus, we will prove the inequality

$$\sigma^2 \leq (x_n - \overline{x})(\overline{x} - x_1). \tag{4}$$

Recall that $n\sigma^2 = \sum_{j=1}^{n} x_j^2 - n\overline{x}^2$. Inequality (4) is established by showing

$$n(x_n - \overline{x})(\overline{x} - x_1) - n\sigma^2 \geq 0. \tag{5}$$

The left hand side of (5) can be written as

$$n\overline{x}(x_n + x_1) - nx_1x_n - \sum_{j=1}^{n} x_j^2 = \left(\sum_{j=1}^{n} x_j\right)(x_n + x_1) - \sum_{j=1}^{n} x_1x_n - \sum_{j=1}^{n} x_j^2$$
$$= \sum_{j=1}^{n}(x_jx_n + x_jx_1 - x_1x_n - x_j^2)$$
$$= \sum_{j=1}^{n}(x_n - x_j)(x_j - x_1)\,.$$

The last expression is clearly greater than or equal to zero, since we have assumed the x's are non-decreasing. This completes the proof of (4) and hence of (2) as well. Note that we have equality in this inequality if and only if all sample values are equal to either x_1 or x_n; that is, if and only if there are at most two sample values.

To prove that the bound is sharper than $R^2/4$, we observe

$$\tfrac{1}{4}(x_n - x_1)^2 - (x_n - \overline{x})(\overline{x} - x_1)$$
$$= \overline{x}^2 - \overline{x}(x_1 + x_n) + x_1x_n + \tfrac{1}{4}(x_n - x_1)^2$$
$$= \overline{x}^2 - \overline{x}(x_1 + x_n) + \tfrac{1}{4}(x_n + x_1)^2$$
$$= \left(\overline{x} - \frac{x_1 + x_n}{2}\right)^2 \ \geq\ 0\,,$$

which proves the claim.

For other useful elementary proofs of statistical inequalities, see [2], which received the George Pólya award.

Acknowledgements: The author wishes to express his gratitude to Dr. Clifford H. Wagner who made several stylistic suggestions and carefully checked the algebra, and to Professor Warren Page who also checked the algebra. The author also thanks the referee and the editor for an improved presentation.

References

[1] Rajendra Bhatia and Chandler Davis, *A better bound on the variance*, The American Mathematical Monthly, **107** (2000), No 4, pp. 353–357.

[2] Warren Page and V.N. Murty, *Nearness relations among measures of central tendency and dispersion: Part 1 and Part 2*, The Two Year College Mathematics Journal **13** (1982), No 5, and **14** (1983), No 1.

Vedula N. Murty
Emeritus Professor of Mathematics and Statistics
PennState, Harrisburg
Middletown, PA, USA 17057
nmvedula@yahoo.com

A Simple Irreducibility Criterion for $f(X^2)$

Natalio H. Guersenzvaig

Let k be any field, and let $f(X)$ be an arbitrary polynomial of $k[X]$ which is irreducible in $k[X]$. A well-known result of Wahlen-Capelli (see [1], p. 212) establishes necessary and sufficient conditions for the irreducibility of $f(g(X))$ in $k[X]$, where $g(X)$ is any polynomial of $k[X]$. The proof of this result is not elementary because it uses the theory of field extensions.

In this short article we establish, with a very elementary proof, necessary and sufficient conditions for the reducibility of $f(X^2)$ in $Z[X]$, where Z denotes an arbitrary unique factorization domain. As an immediate consequence we obtain a simple sufficient condition for the irreducibility of $f(X^2)$ in $Z[X]$.

Theorem 1. *Let $f(X)$ be any non-zero polynomial in $Z[X]$. The following statements are equivalent.*

(i) *$f(X^2)$ is reducible in $Z[X]$.*

(ii) *$f(X)$ is reducible in $Z[X]$ or there exist polynomials $G(X)$, $H(X)$ in $Z[X]$ and a unit u of Z (that is, an invertible element of $Z \setminus \{0\}$) such that*

$$uf(X) \;=\; G^2(X) - XH^2(X)\,. \qquad (\star)$$

Proof. We first suppose that (ii) is true. It is clear that $f(X^2)$ is reducible in $Z[X]$ if $f(X)$ is. Then suppose that $f(X)$ is irreducible in $Z[X]$. Thus, $(\star)$ is true with $H(X) \neq 0$. As a consequence, (i) follows, because $G(X^2)$ and $XH(X^2)$ have degrees of distinct parity and

$$uf(X^2) \;=\; \big(G(X^2) - XH(X^2)\big)\big(G(X^2) + XH(X^2)\big)\,.$$

Now suppose that (i) is true. Assume $f(X)$ is irreducible in $Z[X]$ (otherwise we are done). Then $f(X^2) = g(X)h(X)$, where $g(X)$, $h(X) \in Z[X]$ are not units of Z. Collecting even powers in $g(X)$ and $h(X)$, we obtain

$$g(X) \;=\; G(X^2) + XL(X^2)\,, \qquad h(X) \;=\; H(X^2) + XT(X^2)\,, \qquad (1)$$

for some polynomials G, L, H, and T in $Z[X]$. Hence,

$$\begin{aligned} f(X^2) \;=\; & G(X^2)H(X^2) + X^2L(X^2)T(X^2) \\ & + XG(X^2)T(X^2) + XL(X^2)H(X^2)\,. \end{aligned} \qquad (2)$$

for some polynomials G, L, H, and T in $Z[X]$.

We claim that $L(X)T(X) \neq 0$. We prove this by contradiction. Suppose for example that $L(X) = 0$ (the case $T(X) = 0$ is analogous). Thus, we have

$$f(X^2) - G(X^2)H(X^2) = XG(X^2)T(X^2)\,. \tag{3}$$

Both sides of this equality are zero because, otherwise, they have degrees of different parity. Thus, $T(X) = 0$; whence, $f(X^2) = G(X^2)H(X^2)$; that is, $f(X) = G(X)H(X)$, which contradicts the assumption that $f(X)$ is irreducible in $Z[X]$.

It can be assumed that the greatest common divisor of $G(X)$ and $L(X)$, say $D(X)$, is equal to 1, because, otherwise, we consider the factorization $f(X^2) = g^*(X)h^*(X)$, with $h^*(X) = D(X^2)h(X)$ and

$$g^*(X) = \frac{g(X)}{D(X^2)} = \frac{G(X^2)}{D(X^2)} + X\frac{L(X^2)}{D(X^2)}\,,$$

where such a condition is satisfied. Note that in order to replace $g(X)$ by $g^*(X)$, we need to know that $g^*(X)$ is not a unit of Z. If it were a unit, then $L(X^2) = 0$ from (1) which implies $L(X) = 0$. But this leads to a contradiction, as was shown in the preceding paragraph.

Now, from (2), via the same argument used in (3), we get

$$G(X)T(X) + L(X)H(X) = 0\,, \tag{4}$$

and

$$f(X) = G(X)H(X) + XL(X)T(X)\,.$$

As a consequence,

$$L(X)f(X) = G(X)L(X)H(X) + XL^2(X)T(X)\,.$$

By using (4) this becomes

$$L(X)f(X) = -T(X)\big(G^2(X) - XL^2(X)\big)\,;$$

whence, $L(X)$ is a divisor of $T(X)$ because $G(X)$ and $L(X)$ are coprime polynomials. Thus,

$$f(X) = M(X)\big(G^2(X) - XL^2(X)\big)$$

for some $M(X) \in Z[X]$. But we have assumed that $f(X)$ is irreducible in $Z[X]$. Therefore, $M(X)$ is a unit of Z, and $(\star)$ follows. □

Corollary 1. *Let $f(X)$ be any polynomial of $Z[X]$ which is irreducible in $Z[X]$. Assume that $f(X)$ has leading coefficient A and constant term C. In addition suppose that uA is not a square in Z for each unit u of Z or that AC is not a square in Z. Then*

$f(X^2)$ is irreducible in $Z[X]$.

Remark. If $f(X)$ is detected as irreducible via the well-known Eisenstein's Criterion (see [2, pp. 267-268]), which also works in $Z[X]$ (*mutatis mutandis*), it follows immediately that $f(X^m)$ is irreducible in $Z[X]$ for any positive integer m. However, our result works in cases where Eisenstein's Criterion is inapplicable. As an example of this, we consider the polynomial $f(X) = 3X^2 + 2X + 4 \in \mathbb{Z}[X]$, which is certainly irreducible in $\mathbb{Z}[X]$. Using Corollary 1, we note that $AC = 12$ and ± 3 are not squares in $\mathbb{Z}$. From either of these two facts we have that $f\left(X^{2^m}\right) = 3X^{2^m} + 2X^{2^{m-1}} + 4$ is irreducible in $\mathbb{Z}[X]$ for any positive integer m.

References.

[1] P.M. Cohn, *Algebra*, Vol. 2, John Wiley & Sons, 1977.

[2] W.K. Nicholson, *Introduction to Abstract Algebra*, Wiley, 1999.

Natalio H. Guersenzvaig
Universidad CAECE
Buenos Aires
Argentina
nguersen@fibertel.com.ar