Designs, Codes and Cryptography, 2, 395 (1992)


# Note on a Question by S. Bagchi and B. Bagchi

BERNHARD SCHMIDT
*Mathematisches Institut Giessen, Arndtstr. 2, D-6300 Giessen, F.R. Germany*

Communicated by D. Jungnickel
Received July 16, 1992.

In [1] Bagchi and Bagchi conjectured that one of the hypotheses of their theorem 2(d) is superfluous. This turns out to be true:

PROPOSITION. Let $q \equiv 9 \bmod 16$ be a prime power such that 2 is a fourth power in $F_q$. Then $1 \pm \sqrt{2}$ are nonsquares in $F_q$.

*Proof.* Let $\beta$ be a primitive eighth root of unity in $F_q$ (note that $\beta$ is a nonsquare). Because of

$$(\beta^2 + 1)^2 = \beta^4 + 2\beta^2 + 1 = 2\beta^2$$

we obtain that $(\beta^2 + 1)/\beta$ is a root of 2 which we denote by $\sqrt{2}$. Note that $\sqrt{2}$ is a square and therefore $\beta^2 + 1$ is a nonsquare. Thus the equation

$$(1 + \sqrt{2})\beta(\beta^2 + 1) = (\beta^2 + \beta + 1)(\beta^2 + 1) = \beta(1 + \beta)^2$$

shows that $1 + \sqrt{2}$ is a nonsquare in $F_q$.

Since $(1 + \sqrt{2})(1 - \sqrt{2}) = -1$ this is also true for $1 - \sqrt{2}$.

## Reference

1. S. Bagchi and B. Bagchi, Designs from Pairs of Finite Fields, J.C.T., Series A 52, 51–61 (1989).