Theorem 1. *$QUAD$ is $\mathcal{NP}$-complete.*

Proof. It's easy to see that $QUAD \in \mathcal{NP}$. We show a Karp reduction from 3SAT: Given a 3SAT formula Φ, we construct in polynomial time a system Q of quadratic equations modulo 2 such that Φ is satisfiable if and only if there is a solution for Q.

We first create an auxiliary system Q_0 of *homogeneous cubic monomial* equations[1] over the same variable-set $x_1, ..., x_n$ as Φ. For each clause $C_1, ..., C_m$ of Φ we add one equation to Q_0, as follows: If $C_i = x_{i_1} \vee \neg x_{i_2} \vee x_{i_3}$ we add the equation

$$(1 - x_{i_1}) \cdot x_{i_2} \cdot (1 - x_{i_3}) = 0 \,,$$

and more generally (i.e., for other patterns of negating the three variables in C_i), for $b \in [3]$, we replace x_{i_b} with the arithmetic term $(1 - x_{i_b})$ and replace $\neg x_{i_b}$ with the arithmetic term x_{i_b}, then multiply the three arithmetic terms.

Claim 1.1. *There is a satisfying assignment for Φ if and only if there is a solution for Q_0.*

Proof. Each C_i is satisfied by x if and only if the corresponding equation is satisfied by x. Hence, all C_i's are satisfied by x if and only if all equations are satisfied by x. □

To construct Q from Q_0 we add more variables $z_1, ..., z_m$. For each monomial equation $i \in [m]$ in Q_0, we add two equations to Q, as follows: If the initial monomial equation is $(1 - x_{i_1}) \cdot x_{i_2} \cdot (1 - x_{i_3}) = 0$, we add the two equations

$$(1 - x_{i_1}) \cdot x_{i_2} = z_i, \qquad z_i \cdot (1 - x_{i_3}) = 0 \,,$$

and more generally, if the monomial equation has three terms $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3}$ where each ℓ_{i_b} is of the form x_{i_b} or $1 - x_{i_b}$, we add two equations $\ell_{i_1} \cdot \ell_{i_2} = z_i$ and $z_i \cdot \ell_{i_3} = 0$.

The constructions of Q_0 from Φ and of Q from Q_0 can both be done in polynomial-time (going clause-by-clause, mapping each clause to a monomial equation, then each monomial equation to two equations). The main claim is that:

Claim 1.2. *There's a solution for Q_0 if and only if there's a solution for Q.*

Proof. For the $\Rightarrow$ direction, let x such that $Q_0(x) = 0$. We construct a solution for Q as follows: The x-variables are the same, and as for the z-variables, for each monomial equation $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3} = 0$ we define $z_i = \ell_{i_1} \cdot \ell_{i_2}$.

We show that this is a solution for Q. Consider each pair of equations in Q, corresponding to some initial equation $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3}$ in Q_0. The first corresponding equation in Q is $\ell_{i_1} \cdot \ell_{i_2} = z_i$, and it's satisfied by the definition of z_i. The second equation in Q is $z_i \cdot \ell_{i_3} = 0$. Since $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3} = 0$ (because x is a solution for Q_0) at least one of the three terms is zero, hence either $z_i = 0$ or $\ell_{i_3} = 0$, so the second equation is satisfied.

For the $\Leftarrow$ direction, let $x_1, ..., x_n, z_1, ..., z_m$ be a solution for Q. We show that $x_1, ..., x_n$ is a solution for Q_0. Let $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3} = 0$ be an equation in Q_0. We know that there is some value z_i such that the two equations $\ell_{i_1} \cdot \ell_{i_2} = z_i$ and $z_i \cdot \ell_{i_3} = 0$ are satisfied. Plugging the second equation into the third, we know that $\ell_{i_1} \cdot \ell_{i_2} \cdot \ell_{i_3} = 0$. □

Hence there is a solution for Q if and only if there is a solution for Q_0, which happens if and only if Φ is satisfiable. ■

[1] A monomial equation is a single monomial, i.e. $xyz = 0$ for three variables x, y, z.