Solution 1.1

(a) x' and y' are arbitrary two-bit Boolean functions. A two-bit Boolean function is a polynomial in two binary variables over the binary field Z_2, and the most general such polynomial is

$$B(x,y) = a \oplus M_1 x \oplus M_2 y \oplus pxy \ .$$

The four constants in this expression are determined by the action of the Boolean function on the four inputs:

$$\begin{array}{ll} B(0,0) = a & a = B(0,0) \\ B(1,0) = a \oplus M_1 & M_1 = B(0,0) \oplus B(1,0) \\ B(0,1) = a \oplus M_2 \quad \Longleftrightarrow & M_2 = B(0,0) \oplus B(0,1) \\ B(1,1) = a \oplus M_1 \oplus M_2 \oplus p & p = B(0,0) \oplus B(1,0) \oplus B(0,1) \oplus B(1,1) \end{array} \ .$$

Notice that the general two-bit Boolean function is determined by 4 binary parameters, giving 2^4 such functions, as required.

The general form for a two-bit gate follows immediately by letting x' and y' be given by independent two-bit Boolean functions.

(b) A reversible gate must be invertible. In investigating invertibility, we should be thinking of the inputs and ouputs as two-dimensional vectors in the four-element vector space over Z_2. The additive constants a and b have no effect on invertibility, so we can ignore them, i.e., set them to zero. Now let's look at the action of a general gate on the four inputs:

$$\begin{pmatrix} 0 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} \ ,$$
$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \longrightarrow \begin{pmatrix} M_{11} \\ M_{21} \end{pmatrix} \ ,$$
$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} M_{12} \\ M_{22} \end{pmatrix} \ ,$$
$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \longrightarrow \begin{pmatrix} M_{11} \\ M_{21} \end{pmatrix} \oplus \begin{pmatrix} M_{12} \\ M_{22} \end{pmatrix} \oplus \begin{pmatrix} p \\ q \end{pmatrix} \ .$$

The middle two outputs must be different from the zero vector and different from each other; the six possible choices for these two vectors (the columns of M) are neatly summarized in the six matrices given in (b). In two dimensions, making these two vectors different also means they are linearly independent, which implies that

$$\begin{pmatrix} M_{11} \\ M_{21} \end{pmatrix} \oplus \begin{pmatrix} M_{12} \\ M_{22} \end{pmatrix}$$

is the fourth vector in the space. If either p or q is nonzero, the fourth output will be equal to one of the first three outputs, so invertibility requires that $p = q = 0$, i.e., no quadratic terms.

You should remember that this is a neat way to express algebraically the $4! = 24$ permutations of the four 2-bit strings.

(c)

$M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x \\ y \end{pmatrix}$	identity
$M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} y \\ x \end{pmatrix}$	bit SWAP
$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x \\ x \oplus y \end{pmatrix}$	CNOT with first bit as control and second as target
$M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x \oplus y \\ y \end{pmatrix}$	CNOT with first bit as target and second as control
$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} x \oplus y \\ x \end{pmatrix}$	CNOT with first bit as control and second as target, followed by bit SWAP
$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} x \\ y \end{pmatrix} \longrightarrow \begin{pmatrix} y \\ x \oplus y \end{pmatrix}$	CNOT with first bit as target and second as control, followed by bit SWAP