First, let me recall the proof idea that the size of a fooling set for a language L provides a lower bound on the size of any NFA accepting L.

Let $\{(x_i, y_i) \mid i = 1, 2, \ldots, n\}$ be a fooling set for the language L (i.e., for any i, $x_i y_i$ is in L and for any $i \neq j$, $x_i y_j$ is not in L **or** $x_j y_i$ is not in L). Let M be an NFA for L. Since the string $x_i y_i$ ($i = 1, 2, \ldots, n$) is in L, there is an accepting computation of M on $x_i y_i$; let p_i be the state on this computation that is reached after reading x_i, i.e., we have

$$q_0 \xrightarrow{x_i} p_i \xrightarrow{y_i} r_i,$$

where r_i is an accepting state of M and q_0 is its initial state. Then, the states $p_1, p_2, \ldots, p_n$ must be pairwise distinct because otherwise we would have

$$q_0 \xrightarrow{x_i} p_i = p_j \xrightarrow{y_j} r_j(acc),$$

and

$$q_0 \xrightarrow{x_j} p_j = p_i \xrightarrow{y_i} r_i(acc),$$

which would contradict the assumption that the set $\{(x_i, y_i) \mid i = 1, 2, \ldots, n\}$ is a fooling set for L.

Well, in our case we had a fooling set

$$\mathcal{F} = \{(x_{ki}, y_{ki}) \mid k = 0, 1, \ldots, n-1,\ i = 0, 1, \ldots, 2n-1\},$$

where (x_{ki}, y_{ki}) is the i-th pair in $\mathcal{B}_k$ for $i \notin \{n-1, 2n-1\}$, and it is the first (the second) pair in $\mathcal{C}_k$ for $i = n-1$ (for $i = 2n-1$, respectively); let me recall that:

$$\mathcal{B}_k = \{(b^k a^i, a^{2n-2-i} b^{n-1-k}) \mid i = 0, 1, \ldots, 2n-2 \text{ and } i \neq n-1\},$$

and

$$\mathcal{C}_k = \{(b^k a^{n-1}, b^{n-1} a^{2n-2} b^{n-1-k}), (b^k a^{2n-2} b^{n-1}, a^{n-1} b^{n-1-k})\}.$$

Now, let M be any NFA for our language $shift(L)$. Let p_{ki} be the state on an accepting computation of M on $x_{ki} y_{ki}$ that is reached after reading x_{ki}. Since $\mathcal{F}$ is a fooling set for $shift(L)$, such p_{ki} must exist and must be pairwise distinct. Our aim is to prove that the initial state of M must be different from any state p_{ki}, which will follow that M must have at least $2n^2 + 1$ states.

Let q_0 be the initial state of M. We first show that it must be different from any state p_{ki} with $k > 0$. To do this, note that the string $a^{2n-2} b^{n-1}$ is in $shift(L)$, and so must be accepted (from q_0). Suppose that $q_0 = p_{ki}$ for some $k > 0$ and some i. Then we have:

$$q_0 \xrightarrow{x_{ki}} p_{ki} = q_0 \xrightarrow{a^{2n-2} b^{n-1}} acc$$

which follows that the string $x_{ki} a^{2n-2} b^{n-1}$ is also accepted. But $x_{ki} = b^k u$ for a string u and the string $b^k u a^{2n-2} b^{n-1}$ is not in $shift(L)$ if $k > 0$. So, we have a contradiction.

It remains to prove that q_0 is different from any p_{0i}. To do this we will have to slightly modify the set $\mathcal{B}_0$, so let

$$\mathcal{B}_0 = \{(a^{n-1}b^{n-1}a^i, a^{2n-2-i}b^{n-1}) \mid i = 0, 1, \ldots, 2n-2, i \neq n-1\}$$

(instead of the previous $\mathcal{B}_0 = \{(a^i, a^{2n-2-i}b^{n-1}) \mid i = 0, 1, \ldots, 2n-2, i \neq n-1\}$). The new set $\mathcal{F}$ will still be a fooling set for $shift(L)$:

* the concatenation of pairs in new $\mathcal{B}_0$ is in $shift(L)$,
* the concatenation of two different pairs in new $\mathcal{B}_0$ works as before
* the concatenation of a pair in new $\mathcal{B}_0$ and a pair in $\mathcal{C}_0$ will be OK as well
* the concatenation of a pair in new $\mathcal{B}_0 \cup \mathcal{C}_0$ and a pair of $\mathcal{B}_k \cup \mathcal{C}_k$ for $k > 0$ used the second part of the former pair which we do not change.

OK, now, we will be able to prove that q_0 is different from any p_{0i}, where p_{0i} are states corresponding to the new pairs (x_{0i}, y_{0i}). To do this note that the string $ba^{2n-2}b^{n-2}$ is in $shift(L)$ and so must be accepted by M. Suppose that $q_0 = p_{0i}$ for some i. Then we have

$$q_0 \xrightarrow{x_{0i}} p_{0i} = q_0 \overset{ba^{2n-2}b^{n-2}}{\longrightarrow} acc$$

which follows that the string $x_{0i}ba^{2n-2}b^{n-2}$ is also accepted. But $x_{0i} = a^{n-1}v$ for a string v and the string $a^{n-1}vba^{2n-2}b^{n-2}$ is not in $shift(L)$ (since the only possible shift to be in L is $a^{n-1}b^{n-2}a^{n-1}vba^{n-1}$, but after reading $a^{n-1}b^{n-2}$ we are in state 1 and then cannot read a^{n-1}). So, we again have a contradiction.

This follows that the initial state of M must be different from any of $2n^2$ states p_{ki}, and so the NFA M needs at least $2n^2 + 1$ states.