Composition note: The solutions here are not self-explanatory, but assume that the reader is looking at the problem prompts at the same time.

1. The next Hamming code is $(15, 11)$ [as discussed in the homework]. The E matrix is 15×11, the D matrix is 11×15, and the C matrix is 4×15. As always, $DE = I$ (because decoding undoes encoding) and $CE = 0$ (because a valid codeword should check to zero).

2. The next Hamming code is $(31, 26)$. The E matrix is 31×26, the D matrix is 26×31, and the C matrix is 5×31. As always, $DE = I$ and $CE = 0$. [For any integer $k \geq 2$, there is a $(2^k - 1, 2^k - 1 - k)$ Hamming code, that encodes $(2^k - 1 - k)$-bit messages into $(2^k - 1)$-bit codewords by appending k check bits. The $(7, 4)$ Hamming code is the $k = 3$ case.]

3. First, $\phi(n) = (p - 1)(q - 1) = 22 \cdot 28 = 616$. We compute the greatest common divisor of $\phi(n)$ and e using the Euclidean algorithm:

$$\begin{aligned} 616 &= 41 \cdot 15 + 1, \\ 15 &= 15 \cdot 1 + 0. \end{aligned}$$

Because $GCD(\phi(n), e) = 1$, e is a valid encryption key. Now we use the extended Euclidean algorithm to compute the inverse of e modulo $\phi(n)$. We start by rewriting the second-to-last equation above, as

$$1 = 1 \cdot 616 + (-41) \cdot 15.$$

And we're already done, because this example was so short. The inverse of 15 modulo 616 is -41, or equivalently $616 - 41 = 575$. Thus $d = 575$.

4. There are $C(n, 2)$ possible games. Each game has two possible outcomes (p_i beats p_j, or p_j beats p_i). So there are $2^{C(n,2)}$ possible summaries.

5. There are $C(n, 2)$ games. Each game has 42 possible outcomes (p_i scores 21 and p_j scores somewhere between 0 and 20, or vice-versa). So there are $42^{C(n,2)}$ possible summaries.

6. You wish to compute the probability that no error occurred, given that you received a valid codeword. The probability that no error occurred is $(0.99)^8$. In a valid codeword, there is either an error in both the first and fifth bits, or no error in either of these bits. In other words, the errors in the first and fifth bits must match. Similarly, the errors in the second and sixth bits must match, the errors in the third and seventh bits must match, and the errors in the fourth and eighth bits must match. There is $C(4, 0) = 1$ way to have errors on zero bits, with probability $(0.99)^8$. There are $C(4, 1) = 4$ ways to have errors in one matched pair of bits, each with probability $(0.99)^6(0.01)^2$. There are $C(4, 2) = 6$ ways to have errors in two matched pairs of bits, each with probability $(0.99)^4(0.01)^4$. There are $C(4, 3) = 4$ ways to have errors in three matched pairs of bits, each with probability $(0.99)^2(0.01)^6$. There is $C(4, 4) = 1$ way to

have errors in all four matched pairs of bits, with probability $(0.01)^8$. Hence

$$\begin{aligned}
p(\text{no error}|\text{valid}) &= \frac{p(\text{no error} \cap \text{valid})}{p(\text{valid})} \\
&= \frac{p(\text{no error})}{p(\text{valid})} \\
&= \frac{(0.99)^8}{\binom{4}{0}(0.99)^8 + \binom{4}{1}(0.99)^6(0.01)^2 + \binom{4}{2}(0.99)^4(0.01)^4 + \binom{4}{3}(0.99)^2(0.01)^6 + \binom{4}{4}(0.01)^8} \\
&= \frac{(0.99)^8}{\sum_{k=0}^{4}\binom{4}{k}((0.01)^2)^k((0.99)^2)^{4-k}} \\
&= \frac{(0.99)^8}{((0.01)^2 + (0.99)^2)^4}.
\end{aligned}$$

[By the way, the answer is about 0.9996.]