In Lemma 2 you prove that the polynomial J, corresponding to 11001, is irreducible over $GF(2)$. Then in Lemma 3 you prove that $GF(2)/(J)$ is isomorphic to $GF(16)$. (In general, when J is an irreducible polynomial of degree d, then $GF(2)/(J)$ is isomorphic to $GF(2^d)$.)

Then in Lemma 4 you prove that all elements in $GF(16)^*$ (thus different from 0) satisfy $x^15 = 1$. (In general, all elements in $GF(2^d)^*$ satisfy $x^{2^d-1} = 1$.) This is just a general result.

The next important fact is to compute the order of the roots of J in the multiplicative group $GF(16)^*$. And it turns out, that this order is 15. Hence, in this special example, they are of maximal order. In general it is not important that they are of maximal order. In general, we get that the order (in the cyclic group $GF(2^d)^*$) of the roots of an irreducible polynomial of degree d over $GF(2)$ is a divisor of $2^d - 1$, but it is not a divisor of $2^k - 1$ for $k < d$. Moreover, the orders of two different roots of the same irreducible polynomial coincide.

Finally, in Lemma 6 you prove that when $\alpha \in GF(16)$ is a root of J, then also α^{2^k} is a root of J. This follows also immediately in general situations, when applying the Frobenius Automorphism: $\psi : GF(2^d) \to GF(2^d)$, $x \mapsto \psi(x) := x^2$. It is an automorphism of $GF(2^d)$ which does not change any element of the prime field $GF(2)$.

How to generalize this proof? First it is very easy to generalize it to other irreducible polynomials J. Since these polynomials come from 01-sequences and we want to partition a line we always assume that the sequences start with a 1, whence the polynomial J starts always with the constant term 1, thus $J = 1 + \ldots$ and consequently $J(0) = 1$.

In general for polynomials J such that $J(0) \neq 0$ the exponent (or the order) of J is defined to be the smallest non-negative integer e, such that J is a divisor of $x^e - 1$. In other words, the exponent of J is

$$\min \{e \in \mathbb{N} \mid J \text{ is a divisor of } \; x^e - 1\}.$$

If moreover J is a monic, irreducible polynomial of degree d with $J(0) \neq 0$, then the following holds.

– The exponent of J is the order of any root of J in the multiplicative $GF(2^d)^*$.

– The exponent of J is a divisor of $2^d - 1$, but not a divisor of $2^k - 1$ for $k < d$. Hence, we can compute the set of all exponents which can occur as exponents of such polynomials of degree d.

– The polynomial J is a divisor of $x^n - 1$ if and only if the exponent of J is a divisor of n.

For that reason it is possible to generalize this approach for irreducible polynomials J of degree d. Lemma 2 is satisfied by assumption, Lemma 3 yields the field $GF(2^d)$. Lemma 4 must be generalized to $GF(2^d)$. Lemma 5 reads as follows: The order of any root of J equals the exponent of J. Lemma 6 is also clear.

How to formulate the Theorem. Let J be an irreducible polynomial coming from a 01-sequence, such that $J(0) \neq 0$, J is of degree d and exponent e, and there are exactly k summands in J different from 0 (i.e. there are exactly k entries equal to 1 in the 01-sequence corresponding to J). Then, any tiling of the line by the pattern corresponding to J and its binary augmentations has a length that is a multiple of lcm (k, e).

In the Johnson problem $k = 3$ is a divisor of $e = 15$. But there exist situations, where we we have to consider the least common multiple. For instance consider the sequence 1101. Hence $J(x) = 1 + x + x^3$, which is irreducible, of degree $d = 3$ and exponent $e = 7$ and has $k = 3$ components 1. Thus lcm $(k, e) = 21$. Here is a tiling of shortest length:

```
1101
  1010001
     1000100000001
      1000100000001
       1000100000001
            1101
              1010001
```

It is still possible to generalize this approach by considering polynomials J which are not irreducible, but still with the natural property $J(0) \neq 0$. Then J can be decomposed into irreducible polynomials over $GF(2)$ which don't vanish at 0. Then the following can be useful.

– If φ is an irreducible polynomial over $GF(2)$, $\varphi(0) \neq 0$, and if n is a positive integer, then the exponent of φ^n equals $e2^t$, where e is the exponent of φ and t is the minimum of all positive integers r, such that $p^r \geq n$. In other words

$$t = \text{min } \{r \in \mathbb{N} \mid p^r \geq n\}.$$

– If J is the product of $\varphi_i^{n_i}$ for $i = 1, \ldots, s$ then the exponent of J is the least common multiple of the exponents of $\varphi_i^{n_i}$.

– The polynomial J is a divisor of $x^n - 1$ if and only if the exponent of J is a divisor of n.

Then also in this situation the generalized version of the Theorem holds.

More information about exponents of polynomials can be found in R. Lidl and H. Niederreiter, Finite Fields. Addison-Wesley Publishing Company. Encyclopedia of Mathematics and its Applications Nr. 20, (1983).