Problem of the Month

Solution to Problem 7: April 2023

(a) Suppose $\boldsymbol{a}$ and $\boldsymbol{b}$ are elements in A_n and that $d(\boldsymbol{a}, \boldsymbol{b}) = k$ for some k. If $k = 0$, then $\boldsymbol{a} = \boldsymbol{b}$, so their distance in the graph is also 0.

Otherwise, $\boldsymbol{a}$ and $\boldsymbol{b}$ differ at exactly k coordinates $i_1, i_2, \ldots, i_k$ where $i_1 < i_2 < \cdots < i_k$. Using the notation introduced in the problem statement, we mean that $\boldsymbol{a}[i] \neq \boldsymbol{b}[i]$ if i is in the list $i_1, i_2, \ldots, i_k$ and $\boldsymbol{a}[i] = \boldsymbol{b}[i]$ otherwise. Notice that the function $g(x) = 1 - x$ has the property that $g(0) = 1$ and $g(1) = 0$, so g switches 1 and 0. We will now define a sequence $\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_k$ of elements in A_n. Informally, $\boldsymbol{a}_1$ is obtained from $\boldsymbol{a}$ by leaving all coordinates alone except $\boldsymbol{a}[i_1]$, which gets changed from 0 to 1 or 1 to 0 as appropriate. Continuing, $\boldsymbol{a}_2$ is obtained from $\boldsymbol{a}_1$ by leaving all coordinates alone except $\boldsymbol{a}_1[i_2]$, which gets switched, and this continues for $\boldsymbol{a}_3$, $\boldsymbol{a}_4$, and so on. More formally, for each $m \geq 1$ with $1 \leq m \leq k$ we define $\boldsymbol{a}_m$ as follows.

- $\boldsymbol{a}_m[i] = \boldsymbol{a}[i]$ if i is not in the list $i_1, i_2, \ldots, i_k$.
- $\boldsymbol{a}_m[i] = g(\boldsymbol{a}[i])$ for each i in the list $i_1, i_2, \ldots, i_m$.
- $\boldsymbol{a}_m[i] = \boldsymbol{a}[i]$ for each i in the list $i_{m+1}, i_{m+2}, \ldots, i_k$.

By construction, the list $\boldsymbol{a}, \boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_{k-1}, \boldsymbol{a}_k$ is a list in which every pair of elements differ at exactly one coordinate. Moreover, the list is that which is generated by changing the coordinates of $\boldsymbol{a}$ that differ from those of $\boldsymbol{b}$ one at a time, from leftmost to rightmost. This means $\boldsymbol{b} = \boldsymbol{a}_k$, and the above is a walk from $\boldsymbol{a}$ to $\boldsymbol{b}$. There are $k + 1$ vertices in this walk, so there are k edges.

We have constructed a walk from $\boldsymbol{a}$ to $\boldsymbol{b}$ in the natural graph of A_n that has length k, which means the distance from $\boldsymbol{a}$ to $\boldsymbol{b}$ in the natural graph is at most k. To see that it is at least k, we suppose $\boldsymbol{a}, \boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_{m-1}, \boldsymbol{b}$ is a walk in the natural graph of A_n of length m for some m. Since there are m vertices in this walk in addition to $\boldsymbol{a}$ and two vertices have an edge between them exactly when they differ at exactly one coordinate, the total number of coordinates at which $\boldsymbol{a}$ and $\boldsymbol{b}$ (the ends of the walk) can differ is at most m. Since we know that they differ at exactly k coordinates, we must have that $m \geq k$. This means that any walk from $\boldsymbol{a}$ to $\boldsymbol{b}$ in the natural graph of A_n has at least k edges.

We have shown that the distance in the natural graph between $\boldsymbol{a}$ and $\boldsymbol{b}$ is at least k and at most k, which means it is exactly k.

(b) For convenience, in the solution to this part and the solution to part (c), we will refer to a two element subset as a *pair*. Since $d(\boldsymbol{a}, \boldsymbol{b}) = d(\boldsymbol{b}, \boldsymbol{a})$ for any elements $\boldsymbol{a}, \boldsymbol{b} \in A_n$, we will say that $d(\boldsymbol{a}, \boldsymbol{b})$ is *the Hamming distance of the pair* $\{\boldsymbol{a}, \boldsymbol{b}\}$ or *the pair* $\{\boldsymbol{a}, \boldsymbol{b}\}$ *has Hamming distance* $d(\boldsymbol{a}, \boldsymbol{b})$, and possibly other similar things depending on the grammar in that particular sentence. Similarly, we might say that $\{\boldsymbol{a}, \boldsymbol{b}\}$ *has distance* k *in a graph* to mean that the distance between the vertices labelled by $\boldsymbol{a}$ and $\boldsymbol{b}$ is k in that graph.

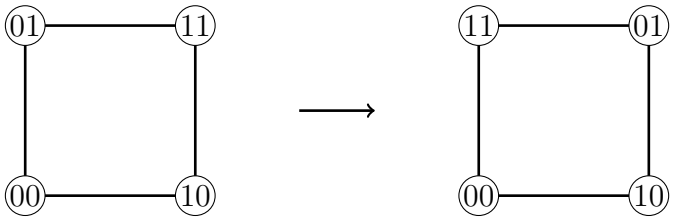
For a fixed element $\boldsymbol{a} \in A_n$, an element $\boldsymbol{b} \in A_n$ satisfies $d(\boldsymbol{a}, \boldsymbol{b}) = k$ exactly when it differs from $\boldsymbol{a}$ at exactly k coordinates. There are n coordinates in total, so there are

$\binom{n}{k}$ possible choices of k coordinates that could be different from $\boldsymbol{a}$. Therefore, for a fixed element $\boldsymbol{a} \in A_n$, there are exactly $\binom{n}{k}$ elements $\boldsymbol{b} \in A_n$ with the property that $d(\boldsymbol{a}, \boldsymbol{b}) = k$. There are 2^n elements in A_n and each $\boldsymbol{a} \in A$ belongs to exactly $\binom{n}{k}$ pairs with a Hamming distance of k. This gives a total of $2^n \times \binom{n}{k}$ pairs. However, this total counts every pair twice, once for each of its two elements. Thus, the number of pairs in A_n with a Hamming distance of k is $\frac{1}{2}2^n\binom{n}{k} = 2^{n-1}\binom{n}{k}$.

(c) Denote by E_n the set of pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from A_n satisfying $d(\boldsymbol{a}, \boldsymbol{b}) = 1$. From part (b), there are $2^{n-1}\binom{n}{1} = n2^{n-1}$ pairs in E_n. In the relabelled natural graph of A_n, we want the distances of the pairs in E_n to be equally distributed among all possible distances in the graph. There are n possible distances between distinct vertices in the graph, so the fact that $n2^{n-1}$ is a multiple of n is a good sign.

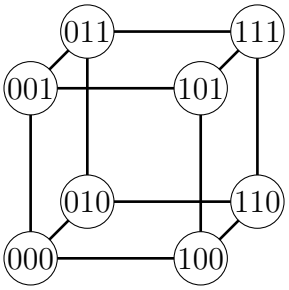
We want to permute the elements of A_n in such a way that for each k from 1 through n, exactly $\dfrac{n2^{n-1}}{n} = 2^{n-1}$ pairs in E_n have a distance of k in the relabelled graph.

There are many ways to do this. The approach given here is inductive, starting by examining A_2. Consider the example from the problem statement. In that example, 01 and 11 were switched and 00 and 10 stayed the same



Although it is not very interesting in A_2, there is an observation we can make that will generalize. The vertices that are connected by horizontal edges in the diagram of the natural graph of A_2 remain connected by an edge after permuting. The vertices in the top change order but their distance apart does not change. Meanwhile, the vertices that are connected by a vertical edge are moved to occupy opposite corners of the square so their distance goes from 1 to 2. While this is only an increase of 1, it will be useful going forward to think of the vertices connected by vertical edges as having gone from as close together as possible (connected by an edge) to as far apart as possible.

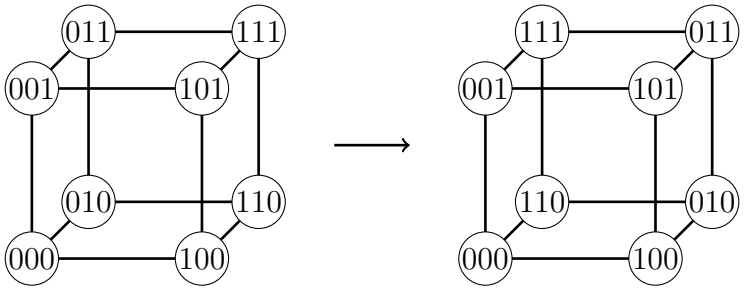
Now consider the natural graph of A_3, which is pictured below.



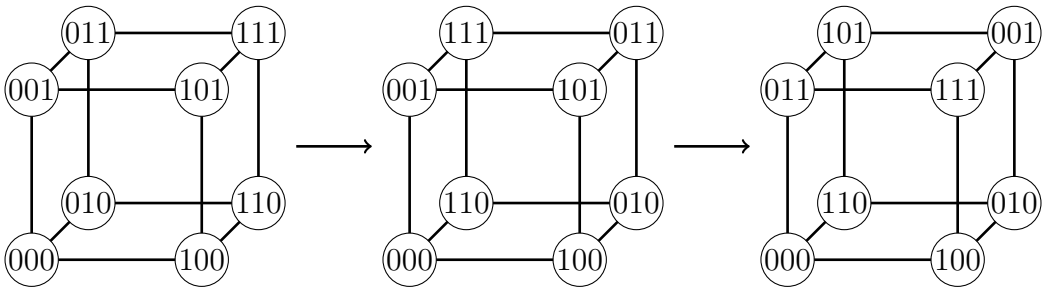
There are 12 edges in the graph. After permuting the labels of the graph, we want $\frac{12}{3} = 4$ pairs of adjacent vertices to be sent to adjacent vertices, 4 pairs of adjacent vertices to be sent to vertices with a distance of 2, and 4 pairs of adjacent vertices to be sent to vertices with a distance of 3.

Looking at the diagram, we can think of the natural graph of A_3 as being composed of two copies of the natural graph of A_2 laid horizontally on top of each other. The labelling also has some coherence with the labelling of A_2. First, label the bottom and top square as if they were copies of the natural graph of A_2, making sure to label vertically-adjacent vertices in the same way. Next, append a 0 to the right of every label in the bottom layer and append a 1 to the right of every label in the top layer.

To permute the labels in the way we want, we will first perform the same permutation on each layer as we did in A_2. In each layer, this moves two pairs of labels from adjacent vertices so that they are at a distance of 2. There are also two pairs of adjacent vertices in each layer that remain adjacent after permuting. The four pairs of vertically-adjacent vertices will remain vertically adjacent because we will have performed the exact same permutation in each layer. At this point, the labels on four pairs of adjacent vertices have been sent to vertices that are 2 apart and the other 8 pairs of labels remain on adjacent vertices. The diagram below shows what we have done so far:



The second and final step is to swap the corners in the top layer. This will have the effect of moving the labels on vertically-adjacent vertices to be as far apart as possible. In a "cube", this means they will end up at opposite ends of a "space diagonal". Swapping the corners in a layer preserves the distance between all pairs of vertices in that layer. This means the net effect of the second step is to move four pairs of adjacent vertices so that they are at a distance of 3. The overall effect is shown below:



In the table below, the first column has the 12 pairs from E_3 and the second column has the distance of the corresponding pair in the relabelled graph.

$\{\boldsymbol{a}, \boldsymbol{b}\}$	new distance
$\{000, 001\}$	3
$\{000, 010\}$	2
$\{000, 100\}$	1
$\{001, 011\}$	2
$\{001, 101\}$	1
$\{010, 011\}$	3
$\{010, 110\}$	1
$\{011, 111\}$	1
$\{100, 101\}$	3
$\{100, 110\}$	2
$\{101, 111\}$	2
$\{110, 111\}$	3

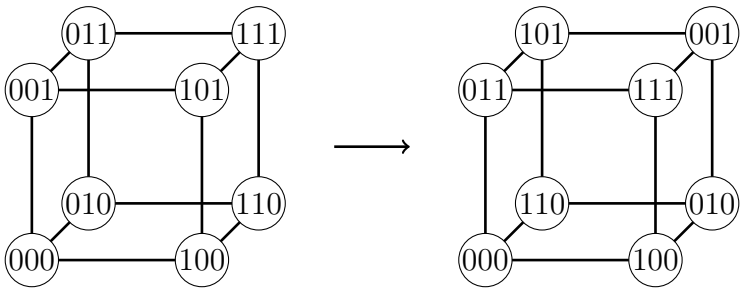
As n grows, the natural graph of A_n gets harder and harder to draw in a useful way, so we need some notation to help translate the geometric idea into symbols. First, we will clarify what we actually want.

Suppose f is a function with *domain* A_n and *codomain* A_n. This means f is a function that takes elements of A_n as input and also outputs elements of A_n. When we talk about a permutation of A_n, we really mean a function f with domain and codomain both equal to A_n that is a *bijection*. For a brief discussion about what a bijection is, you can consult Appendix 1 from the solution to the February 2023 problem. In the context of this solution, a function from A_n to A_n is a permutation if every possible output is attained by exactly one input. For example, the function f with domain and codomain A_2 given by

$$\begin{aligned} f(00) &= 11 \\ f(01) &= 01 \\ f(10) &= 00 \\ f(11) &= 10 \end{aligned}$$

is a bijection from A_2 to A_2. Every possible output is attained (the four elements of A_2 appear on the right side of the displayed equations above) and no output is attained more than once. If you think about it, every way to order the elements of A_2 (a permutation) corresponds to exactly one such function: choose an order of the elements, then write them in that order in the second column above. It will not be important for this solution, but it might help you to understand this connection if you convince yourself that there are exactly $4! = 24$ bijections from A_2 to itself.

A rearrangement of the labels in the natural graph of A_n can be thought of as a bijection from A_n to itself. If f is such a function, then $f(\boldsymbol{a})$ is equal to the original label of the vertex to which the label $\boldsymbol{a}$ is sent by the permutation. For example, the permutation for A_3 corresponding to the relabelling from earlier (shown below)



is given by

$$\begin{aligned} f(000) &= 000 \\ f(001) &= 111 \\ f(010) &= 110 \\ f(011) &= 001 \\ f(100) &= 100 \\ f(101) &= 011 \\ f(110) &= 010 \\ f(111) &= 101 \end{aligned}$$

For example, the fourth of the displayed equations above is $f(011) = 001$ because in the second diagram 011 appears where 001 originally appeared.

This is an important observation because we can now recognize distance in the relabelled graph as a Hamming distance. The distance between $\boldsymbol{a}$ and $\boldsymbol{b}$ in the relabelled graph is equal to the distance between $f(\boldsymbol{a})$ and $f(\boldsymbol{b})$ in the original graph. By part (a), this means the distance between $\boldsymbol{a}$ and $\boldsymbol{b}$ in the relabelled graph is equal to $d(f(\boldsymbol{a}), f(\boldsymbol{b}))$.

We can now formally articulate what we seek. For each n, we would like a function f_n with domain and codomain both equal to A_n with the following properties.

- f_n is a permutation of A_n (a bijection).
- Among the $n2^{n-1}$ pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from E_n, $d(f_n(\boldsymbol{a}), f_n(\boldsymbol{b}))$ takes on each value from 1 through n exactly 2^{n-1} times.

It may be a good idea to digest what has been said so far, possibly going back to see how this applies to A_2 and A_3.

We can now define f_n for each n, but the definition will be recursive, so we need a bit more notation. For an element $\boldsymbol{a}$ in A_n where $n \geq 1$, we will write $\boldsymbol{a}|0$ to mean the element of A_{n+1} that is obtained by appending a 0 to the right end of $\boldsymbol{a}$. For example, $00110|0 = 001100$. Similarly, $\boldsymbol{a}|1$ is the element of A_{n+1} obtained by appending 1 to the right end of $\boldsymbol{a}$. Also, we will denote by $\overline{\boldsymbol{a}}$ the element of A_n obtained by changing every

coordinate of $\boldsymbol{a}$ from 0 to 1 or 1 to 0, as appropriate. For example, if $\boldsymbol{a} = 0010111$, then $\overline{\boldsymbol{a}} = 1101000$.

Starting with $n = 1$ (which we have not addressed up to this point) we will let $f_1(\boldsymbol{a}) = \boldsymbol{a}$. That is, $f_1(\boldsymbol{a})$ is the *identity* function. The elements of A_1 are 0 and 1, and $f_1(0) = 0$ and $f_1(1) = 1$. We now continue recursively. For $n \geq 1$, we define f_{n+1} from f_n as follows.

- If $\boldsymbol{a} \in A_{n+1}$ is of the form $\boldsymbol{b}|0$ for some $\boldsymbol{b} \in A_n$, then $f_{n+1}(\boldsymbol{a}) = f_n(\boldsymbol{b})|0$.
- If $\boldsymbol{a} \in A_{n+1}$ is of the form $\boldsymbol{b}|1$ for some $\boldsymbol{b} \in A_n$, then $f_{n+1}(\boldsymbol{a}) = \overline{f_n(\boldsymbol{b})}|1$.

Notice that the above instructions indeed explain how to evaluate f_{n+1} at every element of A_{n+1} because each element of A_{n+1} can be constructed in exactly one way by appending either a 0 or a 1 to the right of an element from A_n. As an example, we will determine exactly what f_2 does to each element in A_2. For 00, we have to use the rule in the first bullet point because the rightmost digit is 0. $f_1(0) = 0$, so we have that $f_2(00) = 00$. Since the second digit of 10 is also 0 and $f_1(1) = 1$, we get that $f_2(10) = 10$. For 01, we have to use the rule in the second bullet point. This means $f_2(01) = \overline{f_1(0)}|1 = \overline{0}|1 = 11$. Finally, $f_2(11) = \overline{f_1(1)}|1 = \overline{1}|1 = 01$. This is exactly the function from A_2 to itself discussed earlier. We leave it as an exercise to verify that f_3 is exactly the permutation of A_3 discussed earlier.

We can now prove by induction that f_n does what we want for every n. Before doing that, we will discuss how this function corresponds to the geometric idea from earlier. The elements in A_{n+1} can be obtained by taking each element of A_n and appending a 0 to the right and a 1 to the right, in a way getting two elements in A_{n+1} from every element in A_n. By this reasoning, A_{n+1} can be thought of as two copies of A_n: elements ending in 0 and elements ending in 1. If you look at the natural graph of A_3 above, these two copies are exactly the "bottom" and the "top" squares. The way f_{n+1} is defined is to operate differently on the two copies of A_n, since how $f_{n+1}(\boldsymbol{a})$ is computed depends on the rightmost digit of $\boldsymbol{a}$. In other words, it depends on which copy of A_n $\boldsymbol{a}$ belongs to. If $\boldsymbol{a}$ has a rightmost digit of 0, then f_{n+1} essentially does what f_n did. This corresponds to the bottom face of the cube being permuted exactly as the square was. If the rightmost digit of $\boldsymbol{a}$ is 1, then $\boldsymbol{a}$ is in the other copy, corresponding to the top face of the cube in the case of A_3. In this situation, we apply f_n to the element of A_n obtained by removing the last digit, just as we would if the rightmost digit were 0. However, we then switch every digit, and this corresponds to "swapping the diagonals" in A_3. Finally, a 1 is appended to the right of the result, which corresponds to making sure that elements in the top of the cube stay in the top of the cube during the permutation.

For $n = 1$, it is an exercise in understanding definitions to see that f_n satisfies the given conditions. We have already established this for $n = 2$, and $n = 3$ can be verified by confirming that f_3 is exactly the permutation from earlier that we verified worked.

We now assume, for some $n \geq 1$, that f_n is a permutation of A_n with the property that among pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from E_n, $d(f_n(\boldsymbol{a}), f_n(\boldsymbol{b}))$ takes on every value from 1 through n exactly 2^{n-1} times. We will show that f_{n+1} is a permutation of A_{n+1} with the property that among pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from E_{n+1}, $d(f_{n+1}(\boldsymbol{a}), f_{n+1}(\boldsymbol{b}))$ takes on every value from 1 through $n + 1$ exactly 2^n times.

To see that f_{n+1} is a permutation, let $\boldsymbol{a} \in A_n$ be arbitrary. Since f_n is a permutation,

there is a unique element $\boldsymbol{b} \in A_n$ such that $f_n(\boldsymbol{b}) = \boldsymbol{a}$ and a unique element $\boldsymbol{c} \in A_n$ such that $f_n(\boldsymbol{c}) = \overline{\boldsymbol{a}}$. Using the definition of f_{n+1}, we have $f_{n+1}(\boldsymbol{b}|0) = f_n(\boldsymbol{b})|0 = \boldsymbol{a}|0$ and $f_{n+1}(\boldsymbol{c}|1) = \overline{f_n(\boldsymbol{c})}|1 = \overline{\overline{a}}|1 = \boldsymbol{a}|1$. Since every element in A_{n+1} is of the form $\boldsymbol{a}|0$ or $\boldsymbol{a}|1$ for some $\boldsymbol{a} \in A_n$, we have shown that every element of A_{n+1} is in the range of f_{n+1}. Now suppose $\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_3, \ldots, \boldsymbol{a}_{2^{n+1}}$ are the elements of A_{n+1} (in some order). We have shown that every element of A_{n+1} appears in the list

$$f_{n+1}(\boldsymbol{a}_1), f_{n+1}(\boldsymbol{a}_2), \ldots, f_{n+1}(\boldsymbol{a}_{2^{n+1}})$$

at least once. There are 2^{n+1} elements in the list above and 2^{n+1} elements in A_{n+1}, so every element of A_{n+1} must appear in the list above exactly once. In other words, f_{n+1} is a permutation of A_{n+1}.

To prove the other fact about f_{n+1}, we will use the fact that $d(\boldsymbol{a}, \boldsymbol{b}) = d(\overline{\boldsymbol{a}}, \overline{\boldsymbol{b}})$ for any $\boldsymbol{a}$ and $\boldsymbol{b}$. It is left as an exercise to verify this.

Suppose k is a positive integer such that $1 \leq k \leq n$. By induction, there are exactly 2^{n-1} pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ in E_n with $d(f_n(\boldsymbol{a}), f_n(\boldsymbol{b})) = k$. If $\{\boldsymbol{a}, \boldsymbol{b}\}$ is one of these 2^{n-1} pairs, we have

$$\begin{aligned} d(f_{n+1}(\boldsymbol{a}|0), f_{n+1}(\boldsymbol{b}|0)) &= d(f_n(\boldsymbol{a})|0, f_n(\boldsymbol{b})|0) \\ &= d(f_n(\boldsymbol{a}), f_n(\boldsymbol{b})) \\ &= k \end{aligned}$$

where the second equality is because the elements in question agree in the last coordinate, so their Hamming distance is equal to the Hamming distance between the elements obtained by removing the rightmost elements. We similarly have that

$$\begin{aligned} d(f_{n+1}(\boldsymbol{a}|1), f_{n+1}(\boldsymbol{b}|1)) &= d(\overline{f_n(\boldsymbol{a})}|1, \overline{f_n(\boldsymbol{b})}|1) \\ &= d(\overline{f_n(\boldsymbol{a})}, \overline{f_n(\boldsymbol{b})}) \\ &= d(f_n(\boldsymbol{a}), f_n(\boldsymbol{b})) \\ &= k \end{aligned}$$

Therefore, there are $2 \times 2^{n-1} = 2^n$ pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from E_{n+1} satisfying $d(f_{n+1}(\boldsymbol{a}), f_{n+1}(\boldsymbol{b})) = k$ for each $1 \leq k \leq n$.

Next, for any $\boldsymbol{a} \in A_n$, we have

$$\begin{aligned} d(f_{n+1}(\boldsymbol{a}|0), f_{n+1}(\boldsymbol{a}|1)) &= d(f_n(\boldsymbol{a})|0, \overline{f_n(\boldsymbol{a})}|1) \\ &= d(f_n(\boldsymbol{a}), \overline{f_n(\boldsymbol{a})}) + 1 \\ &= n + 1 \end{aligned}$$

where the second equality is because we know that the two elements being handed to d have different rightmost coordinates, so their Hamming distance is one more than the Hamming distance between the elements obtained by removing the rightmost coordinates. The third equality is because $\overline{f_n(\boldsymbol{a})}$ and $f_n(\boldsymbol{a})$ differ in all n coordaintes by definition.

There are 2^n elements of A_n, and each pair $\{\boldsymbol{a}|0, \boldsymbol{a}|1\}$ is in E_{n+1}, so we get 2^n pairs from E_{n+1} such that $d(f_{n+1}(\boldsymbol{a}), f_{n+1}(\boldsymbol{b})) = n + 1$. For each k from 1 through $n + 1$, we have found 2^n pairs $\{\boldsymbol{a}, \boldsymbol{b}\}$ from E_{n+1} with the property that $d(f_{n+1}(\boldsymbol{a}), f_{n+1}(\boldsymbol{b})) = k$. This completes the proof.