Beautiful Problems

Alec Lau

Contents

1 Bounding Steps of the Euclidean Algorithm

Proof. Looking at the Euclidean algorithm, we see that the worst case step is if the fewest multipliers are applied, so this points us toward using the Fibonacci sequence to bound this. First we prove that, in Euclid's algorithm, we always have $a_n \geq f_{n+2}$. We use induction on n. Note that the results hold when $n = 0$ and $n = 1$; when $n = 0$ we want $a_0 \geq f_2 = 1$, which is trivial as a_0 is a positive integer. When $n = 1$ we want $a_1 \geq f_3 = 2$, which holds because $a_1 > a_0$. This last inequality holds because a_0 is the residue of a_2 modulo a_1 (or, in the special case a_1 and a_0 are the numbers we begin with, we assume they are different). Now suppose $n \geq 2$. Then a_{n-2} is given us the residue of a_n when divided by a_{n-1}; $a_n = qa_{n-1} + a_{n-2}$. Since $a_n > a_{n-1}$, we have $q \geq 1$ and thus $a_n \geq a_{n-1} + a_{n-2} \geq f_{n+1} + f_n = f_{n+2}$ by induction hypothesis.

Thus if it takes more than 45 divisions, then in the setup we have either x or y is equal to a_n with $n \geq 46$. But according to google we see that $f_{48} > 2^{32}$, thus $a_n \geq f_n + 2 \geq f_{48} > 2^{32}$ which contradicts the assumption. □

2 The Wave Equation on a Riemannian Manifold

Proof. Expanding $(\nabla^2 f)(X,Y)$, we have this equal to $(\nabla(\nabla f))(X,Y)$ by definition. By the definition of ∇, we have this equal to $(\nabla_X(\nabla f))(Y)$. From class and the footnote, we have

$$\nabla_X[\nabla f(Y)] = (\nabla_X(\nabla f))(Y) + \nabla f(\nabla_X Y) \Rightarrow \tag{1}$$

$$(\nabla_X(\nabla f))(Y) = \nabla_X[\nabla f(Y)] - \nabla f(\nabla_X Y) \tag{2}$$

Again by the definition of ∇, the right-hand side then equal to $\nabla_X[\nabla_Y f] - \nabla_{\nabla_X Y} f$, which, again from class and the footnote, is $\nabla_X[Yf] - (\nabla_X Y)f$. Thinking of $[Yf]$ as another function, we have this equal to $X(Yf) - (\nabla_X Y)f$. Thus $(\nabla^2 f)(X,Y) = X(Yf) - (\nabla_X Y)f$.

When we define $\Delta f = \sum_{i,j}^n (g^{-1})^{ij}(\nabla^2 f)(\partial_i, \partial_j)$, we can use our formula proved above to obtain $\sum_{i,j}^n (g^{-1})^{ij}(\partial_i(\partial_j f) - (\nabla_{\partial_i}\partial_j)f) = \sum_{i,j}^n (g^{-1})^{ij}\partial_i(\partial_j f) - (g^{-1})^{ij}(\nabla_{\partial_i}\partial_j)f$. Now we examine the second term, $\sum_{i,j}^n -(g^{-1})^{ij}(\nabla_{\partial_i}\partial_j)f$. We will drop the summation in front and use notation with the understanding that repeated indices are summed over. This term is equal, by definition, to $-(g^{-1})^{ij}\Gamma_{ij}^k \partial_k f$. We have

$$-(g^{-1})^{ij}\Gamma_{ij}^k \partial_k f = -(g^{-1})^{ij}(\frac{1}{2}(g^{-1})^{kl}(\partial_i g_{j,l} + \partial_j g_{il} - \partial_l g_{ij}))\partial_k f \tag{3}$$

$$= \frac{1}{2}(-(g^{-1})^{ij}(g^{-1})^{kl}\partial_i g_{jl} - (g^{-1})^{ij}(g^{-1})^{kl}\partial_j g_{il} + (g^{-1})^{ij}(g^{-1})^{kl}\partial_l g_{ij})\partial_k f \tag{4}$$

$$= (\frac{-1}{2}(-g^{-1})^{ij}(g^{-1})^{kl}\partial_i g_{jl} + \frac{-1}{2}(g^{-1})^{ij}(g^{-1})^{kl}\partial_j g_{il})\partial_k f + \frac{1}{2}((g^{-1})^{ij}(g^{-1})^{kl}\partial_l g_{ij})\partial_k f \tag{5}$$

In examining the first two terms, since the indices are dummy indices, we can relabel indices and rewrite their sum as $-(g^{-1})^{ij}(g^{-1})^{kl}(\partial_i g_{jl})\partial_k f$. We know from the first hint that this is equal to $(\partial_i(g^{-1})^{jk})\partial_k f$, so we now have

$$= (\partial_i(g^{-1})^{jk})\partial_k f + \frac{1}{2}(g^{-1})^{ij}(g^{-1})^{kl}\partial_l g_{ij}\partial_k f \tag{6}$$

$$= (\partial_i(g^{-1})^{jk})\partial_k f + \frac{1}{2}(\partial_l \log(\det g))\partial_k f \tag{7}$$

$$\tag{8}$$

as per the second hint. Then,

$$= (\partial_i(g^{-1})^{jk})\partial_k f + (\partial_l \log(\sqrt{\det g}))\partial_k f \tag{9}$$

$$= (\partial_i(g^{-1})^{jk})\partial_k f + \frac{1}{\sqrt{\det g}}(\partial_l \sqrt{\det g})\partial_k f \tag{10}$$

$$\tag{11}$$

Putting this all together, we have

$$\Delta f = (g^{-1})^{ij}\partial_i(\partial_j f) + (\partial_i(g^{-1})^{jk})\partial_k f + \frac{1}{\sqrt{\det g}}(g^{-1})^{ij}(\partial_l\sqrt{\det g})\partial_k f \tag{12}$$

We now show that this is equal to $\frac{1}{\sqrt{\det g}}\partial_i((g^{-1})^{ij}\sqrt{\det g}\partial_i f)$. Since ∂_i is a derivation, we can use the 'product rule' and apply ∂_i to each of the three terms:

$$\frac{1}{\sqrt{\det g}}\partial_i((g^{-1})^{ij}\sqrt{\det g}\partial_j f) = \frac{1}{\sqrt{\det g}}((\partial_i(g^{-1})^{ij})\sqrt{\det g}\partial_j f + (g^{-1})^{ij}(\partial_i\sqrt{\det g})\partial_j f + (g^{-1})^{ij}\sqrt{\det g}\partial_i\partial_j f) \tag{13}$$

$$= (\partial_i(g^{-1})^{ij})\partial_j f + \frac{1}{\sqrt{\det g}}(g^{-1})^{ij}(\partial_i\sqrt{\det g})\partial_j f + (g^{-1})^{ij}\partial_i(\partial_j f) \tag{14}$$

By relabeling our dummy indices, we see that this is the result we want. □

3 Algebraic Topology with Statistics of Particles

Proof. Starting with $\mathbb{R}^3$, suppose we have two identical particles. We fix one particle at the origin and look at the configuration space of the other particle. We cannot have the two particles in the same place, because of the Pauli Exclusion principle. Other than that, we can have the other particle go to any nonzero point in $\mathbb{R}^3$. In doing a single particle exchange twice, we have the path of the particle during this process is a loop. We have that $\pi_1(\mathbb{R}^3 - \{0\}) \cong \pi_1(S^2)$, because $\mathbb{R}^3 - \{0\}$ can be continuously deformed into S^2 through the map $x \mapsto \frac{x}{|x|}$. Thus $\pi_1(\mathbb{R}^3 - \{0\}) \cong \pi_1(S^2) \cong 0$. Thus, two exchanges give the identity operator. In operator language, this means that, for $\hat{A}$ the exchange operator, $\hat{A}^2\psi = 1\psi$. Thus the eigenvalues of $\hat{A}$ must be equal to 1 or -1, corresponding to bosons and fermions.

In $\mathbb{R}^2$, the same map gives us $\pi_1(\mathbb{R}^2 - \{0\}) \cong \pi_1(S^1) \cong \mathbb{Z}$. Thus $A^2\psi \ncong 0$, so we can allow any eigenvalue of A to be the statistics of the identical particles. □

4 A Surjection between Groups

Proof. We have two generators for G that we shall define as $h : (a, b) \to (-a, b)$ and $j : (a, b) \to (a, -b)$. It is not hard to see that $h^2 = j^2 = e$, the identity of G. There are other rotation operators as generators, but the subgroup generated by rotation operators has torsion, so the image of any homomorphism in H for this subgroup must also be finite. G is infinite on account on two generators f, g with $f : (a, b) \mapsto (a + 1, b), g : (a, b) \mapsto (a, b + 1)$. It is easy to see that the subgroup generated by these two generators is isomorphic to $\mathbb{Z}\times\mathbb{Z}$. This is infinite, so the problems

that could arise from the finiteness of H come from these. Label our surjective homomorphism by φ. Observe that

$$\varphi(hf^x) = \varphi(h)\varphi(f^x) \tag{15}$$

$$\varphi(hf^{-x}) = \varphi(f^x h) = \varphi(f^x)\varphi(h) = \varphi(h)\varphi(f^x) = \varphi(hf^x) \tag{16}$$

Thus $\varphi(hf^x) = \varphi(hf^{-x})$, so $\varphi(h)\varphi(f^x) = \varphi(h)\varphi(f^{-x})$. Left multiplying by $\varphi(h)^{-1}$, we find that $\varphi(f^x) = \varphi(f^{-x}) \Rightarrow \varphi(f)^x = \varphi(f)^{-x}$, so $\varphi(f) = \varphi(f)^{-1}$.

Now notice $\varphi(f) = \varphi(f)^{x+1-x} = \varphi(f)^x\varphi(f)\varphi(f)^{-x} = \varphi(f)^{2x+1}$ for any $x \in \mathbb{Z}$. Thus all odd powers of $\varphi(f)$ map to $\varphi(f)$, and all even powers of $\varphi(f)$ map to the identity of H. Thus H is finite. □

5 Infinite Integers

Proof. In the spirit of the above problems, we want the first digit to satisfy $\overline{a}^3 = 7$. An $a \in \mathbb{Z}/[10]\mathbb{Z}$ that satisfies this is 3, so we let 3 be the first digit of z. Thus, we take $3^3 = 27$. In order to make the second digit equal to 0, we need the second digit in z to be $2 \times \overline{7} = \overline{4}$. This formula [digit]$\times\overline{7}$ as the next digit in z is due to the fact that we want the digit in question of our number to be congruent to 0. This sets the digit of the cube of the current z equal to 0. To illustrate this, consider this calculation:

We have $43^3 = 79507$. We want our next digit $\overline{a}$ to satisfy $(\overline{a} \times 10^2 + 43)^3 \equiv 7 \mod (1000)$. Cubing this out, we find our number equal to $a^3 10^6 + 3a^2 10^4 43 + 3a10^2 43^2 + 43^3$. Let us denote the digit value we're trying to eliminate by d. We only need to consider the latter two terms, as we only care about the third digit for now (if we can't have this equal to zero now, we're screwed). We have now $a554700 + 79507$ (We can see that this new factor of a always has 7 as the last nonzero digit). Thus, we need $a \times 7 = \overline{5}$ in order for this sum to have a third digit of 0. If we set a equal to $\overline{7} \times 7 \times d$, we get $s := \overline{9} \times d$ so that $\overline{s} + \overline{d} = \overline{0}$. Thus, by setting $\overline{a}$ equal to $\overline{7d}$, we get the cube of $\overline{a} \times 10^n$+[our known digits for z, of $n-1$ digits] cancels out our nth digit in the cube.

Example:

$$3^3 = 27 \Rightarrow 2 \times \overline{7} = 4 \rightarrow$$

$$43^3 = 79507 \Rightarrow 5 \times \overline{7} = 5 \rightarrow$$

$$543^3 = 160103007 \Rightarrow 3 \times \overline{7} = 1 \rightarrow$$

$$\vdots$$

$$924422217051543^3 = 7899709545882474340556651700000000000000007^*$$

$$\vdots$$

*This value is courtesy of Wolfram Alpha

Following this algorithm yields a z satisfying $z^3 = 7 \in R$. Thus, such a z exists. □

6 A Quantum Error-Correcting Code

1. For bit-flip errors on the last three qubits, we get $2^3 = 8$ possible states. Since we allow a phase error, a bit flip error, or no error on the first qubit, we multiply 8 by 3 to get 24 possible states for this system.

2. In the stabilizer formalism, for four qubits, to encode one qubit we need to have three generators to ensure the code subspace is a qubit i.e. 2-dimensional: $2^n/2^k = 2$ for $n = 4$ qubits.

3. For a bit flip, acting by Z flips the sign. For a phase flip, acting by X flips the sign. To ensure commutation, we want an even number of X and Z collisions for each index. We want a stabilizer with X in the first index, and a stabilizer Z in the first index as well. We also want a distinct number of Z operators across indices across a distinct set of generators in order to tell which bits have been flipped. Three generators that satisfy these conditions are

$$\text{Generator 1: } Id \otimes Z \otimes Z \otimes Z \tag{17}$$

$$\text{Generator 2: } Z \otimes Z \otimes Id \otimes Z \tag{18}$$

$$\text{Generator 3: } X \otimes X \otimes X \otimes Z \tag{19}$$

   In analyzing data for certain errors, we find

Stabilizer:	1	2	3
Identity	+	+	+
3rd bit flip	-	+	+
1st bit flip	+	-	+
Phase flip	+	+	-
2nd bit flip	-	-	+
4th bit flip	-	-	-
Phase flip & 1st bit flip	+	-	-

   Thus our generators are able to tell which single-bit errors can occur in this system.

4. Looking at the table, we get almost all permutations of 3 values of + and -. We're missing one:

Stabilizer:	1	2	3
"Accidental" error	-	+	-

Looking at the generators, the error that causes these results are a bit flip and phase flip on the 3^{rd} qubit.

7 A Generalization of Shor

1. First we want to find the number of generators. There are 16 qubits, so $2^{16}/2^k = 2$, so $k = 15$. There are 16 possible single-qubit bit flips. Inspired by Shor, there are 4 possible phase flips, for which we need 3 stabilizer generators:

$$X_1 \otimes ... \otimes X_8, X_5 \otimes ... \otimes X_{12}, X_9 \otimes ... \otimes X_{16} \tag{20}$$

We are left with 12 stabilizer generators to determine the 16 bit flips. To ensure commutation, we need an even number of colliding indices of X and Z. What accomplishes this is

$$Z_1 \otimes Z_2, Z_2 \otimes Z_3, Z_3 \otimes Z_4 \tag{21}$$

$$Z_5 \otimes Z_6, Z_6 \otimes Z_7, Z_7 \otimes Z_8 \tag{22}$$

$$Z_9 \otimes Z_{10}, Z_{10} \otimes Z_{11}, Z_{11} \otimes Z_{12} \tag{23}$$

$$Z_{13} \otimes Z_{14}, Z_{14} \otimes Z_{15}, Z_{15} \otimes Z_{16} \tag{24}$$

There are 12 above stabilizer generators, and each bit flip corresponds to a unique comgination of -1 eigenvalues for these generators.

2. Denote $|0_1...0_n 1_1...1_m\rangle$ by $|0^n 1^m\rangle$. We have

$$|0\rangle_L = \frac{1}{4}(|0^4\rangle + |1^4\rangle)^{\otimes 4} \tag{25}$$

$$= \frac{1}{4}[\,|0^{16}\rangle \pm |0^4 1^4 0^8\rangle \pm |1^4 0^{12}\rangle + |1^8 0^8\rangle \pm |0^{12} 1^4\rangle + |0^4 1^4 0^4 1^4\rangle + |1^4 0^8 1^4\rangle \pm |1^8 0^4 1^4\rangle \tag{26}$$

$$\pm |0^8 1^4 0^4\rangle + |0^4 1^8 0^4\rangle + |1^4 0^4 1^4 0^4\rangle \pm |1^{12} 0^4\rangle + |0^8 1^8\rangle \pm |0^4 1^{12}\rangle \pm |1^4 0^4 1^8\rangle + |1^{16}\rangle] \tag{27}$$

where $\pm$ denotes a - when talking about $|1\rangle_L$. Notice that the sign switches under X_L if there are an odd number of switches from $|0^4 0^4 0^4 0^4\rangle$ to whatever tensor term there is. Thus, we can accomplish X_L via

$$X_L = Z \otimes Id^{\otimes 3} \otimes Z \otimes Id^{\otimes 3} \otimes Z \otimes Id^{\otimes 3} \otimes Z \otimes Id^{\otimes 3} \tag{28}$$

which has 4 physical Pauli operators. For Z_L, we seek $Z_L \left|0\right\rangle_L = \left|0\right\rangle_L, Z_L \left|1\right\rangle_L = -\left|1\right\rangle_L$. This begs the use of X. Expanding $\left|1\right\rangle_L$, we get

$$|0^{16}\rangle - |0^4 1^4 0^8\rangle - |1^4 0^{12}\rangle + |1^8 0^8\rangle - |0^{12} 1^4\rangle + |0^4 1^4 0^4 1^4\rangle + |1^4 0^8 1^4\rangle - |1^8 0^4 1^4\rangle \tag{29}$$

$$- |0^8 1^4 0^4\rangle + |0^4 1^8 0^4\rangle + |1^4 0^4 1^4 0^4\rangle - |1^{12} 0^4\rangle + |0^8 1^8\rangle - |0^4 1^{12}\rangle - |1^4 0^4 1^8\rangle + |1^{16}\rangle \tag{30}$$

switching a clump of 4 qubits with X transforms each term into another, which has then a different parity of switches from $|0^4 0^4 0^4 0^4\rangle$ to whatever tensor term there is. Letting

$$Z_L = Id^{\otimes 4} \otimes X^{\otimes 4} \otimes Id^{\otimes 8} \tag{31}$$

we get $Z_L \left|0\right\rangle_L = \left|0\right\rangle_L$ because $\left|0\right\rangle_L$ has all plus signs. We also have $Z_L \left|1\right\rangle_L$

$$|0^4 1^4 0^8\rangle - |0^{16}\rangle - |1^8 0^8\rangle + |1^4 0^{12}\rangle - |0^4 1^4 0^4 1^4\rangle + |0^{12} 1^4\rangle + |1^8 0^4 1^4\rangle - |1^4 0^8 1^4\rangle \tag{32}$$

$$- |0^4 1^8 0^4\rangle + |0^8 1^4 0^4\rangle + |1^{12} 0^4\rangle - |1^4 0^4 1^4 0^4\rangle + |0^4 1^{12}\rangle - |0^8 1^8\rangle - |1^{16}\rangle + |1^4 0^4 1^8\rangle \tag{33}$$

This is equal to $-\left|1\right\rangle_L$ by inspection.

3. X_L and Z_L cannot commute, because we need an odd number of Zs in each clump of 4 qubits in X_L for the correct signs to turn negative, but we need one clump to have all four Z for Z_L, always giving an odd number of anticommuting tensor indices.

8 Real Projective Space

1. We have, for $x \in S^{n-1}$, $x_1^2 + ... + x_n^2 = 1$. For $[x] \in \mathbb{R}P^n$, we have the equivalence $(x_1, ..., x_n) = (-x_1, ..., -x_n)$. Let M be the submanifold of $\mathbb{R}^{n^2}$ given by symmetric $n \times n$ matrices A such that $\mathrm{Tr}(A) = 1$ and $AA = A$. Define a map, for $f_{i,j}([x]) = x_i x_j$, given by

$$\Phi : \mathbb{R}P^{n-1} \to M \tag{34}$$

$$\Phi([x]) \mapsto \Big(f_{i,j}([x]) \Big) \tag{35}$$

We check that the image of Φ is indeed M. We have the kl^{th} entry in $[f_{i,j}([x])][f_{i,j}([x])]$ as

$$f_{k,i}([x]) f_{i,l}([x]) = x_k x_1 x_l x_1 + x_k x_2 x_l x_2 + ... + x_k x_n x_l x_n \tag{36}$$

$$= x_k x_l (x_1^2 + x_2^2 + ... + x_n^2) \tag{37}$$

Thus $[f_{i,j}([x])][f_{i,j}([x])] = [f_{i,j}([x])]$. The trace is easy as well: $\mathrm{Tr}(f_{ij}([x])) = x_1x_1 + ... + x_nx_n = 1$. Furthermore, $[f_{ij}([x])]$ is symmetric, because $x_kx_l = x_lx_k$. This is smooth because the $f_{i,j}$ functions are smooth because multiplication is smooth ($x \mapsto xx^T$). The inverse map is similarly smooth ($xx^T \mapsto x$), so it remains to show that Φ is bijective. We see that $x_ix_j = x_ix_j$ for all $1 \leq i, j \leq n$ if and only if $\{x_i, x_j\} = \{x_i, x_j\}$, except if $\{x_i, x_j\} = \{-x_i, -x_j\}$. However, these antipodal points are identified in $\mathbb{R}P^{n-1}$, Φ is a bijection and thus diffeomorphism.

2. Because $\mathbb{R}P^{n-1}$ is diffeomorphic to M, it suffices to show that M is compact, i.e. closed and bounded. It is bounded because every x_i has $|x_i| \leq 1$, so every entry is at most 1. For closedness, we use the determinant map, which we know is smooth. We have $(A) = \epsilon_{i_1,...,i_n}x_1x_{i_1}...x_nx_{i_n}$, where $\epsilon_{i_1,...,i_n}$ is the Levi-Civita symbol, which is zero if the indices are repeated. Thus the only nonzero terms in the determinant are $x_1^2x_2^2...x_n^2$, with plus or minus signs corresponding the the parity of permutations in the n indices. Since there are equal numbers of odd permutations as even permutations, the determinant of any matrix in M is 0. This is a closed set, and, since the determinant is smooth, M must be closed. Thus M is closed and bounded, i.e. compact.