CS711 Assignment 2

Sankalp Gambhir
180260032

September 19, 2021

Question 1.

(a) *Proof.* Given the polynomial $\mathsf{Trace} : \mathbb{F}_{q^k} \to \mathbb{F}_{q^k}$ defined as

$$\mathsf{Trace}(x) = x + x^q + x^{q^2} + \ldots + x^{q^{k-1}}$$

consider $\forall x$ the quantity $\mathsf{Trace}(x)^q$. By Freshman's Lemma,

$$\begin{aligned}
\mathsf{Trace}(x)^q &= (x)^q + (x^q)^q + (x^{q^2})^q + \ldots + (x^{q^{k-1}})^q \\
&= x^q + x^{q^2} + x^{q^3} + \ldots + x^{q^{k-1}} + x^{q^k} \\
&= x^q + x^{q^2} + x^{q^3} + \ldots + x^{q^{k-1}} + x \\
&= \mathsf{Trace}(x)
\end{aligned}$$

and thus $\mathsf{Trace}(x)$ must be a member of the subfield $\mathbb{F}_q$. So, we can view Trace as a map from $\mathbb{F}_{q^k}$ to the subfield $\mathbb{F}_q$. □

(b) *Proof.* By another application of Freshman's Lemma and the fact that $\alpha^{q-1} = 1 \ \forall \alpha \in \mathbb{F}_q$, we see that Trace is indeed linear as well. We have, $\forall x, y \in \mathbb{F}_{q^k}$ and $\alpha \in \mathbb{F}_q$,

$$\begin{aligned}
\mathsf{Trace}(x+y) &= (x+y) + (x+y)^q + (x+y)^{q^2} + \ldots + (x+y)^{q^{k-1}} \\
&= x + y + x^q + y^q + x^{q^2} + y^{q^2} + \ldots + x^{q^{k-1}} + y^{q^{k-1}} \\
&= \mathsf{Trace}(x) + \mathsf{Trace}(y) \ , \text{ and} \\
\mathsf{Trace}(\alpha x) &= (\alpha x) + (\alpha x)^q + (\alpha x)^{q^2} + \ldots + (\alpha x)^{q^{k-1}} \\
&= \alpha x + \alpha^q x^q + \alpha^{q^2} x^{q^2} + \ldots + \alpha^{q^{k-1}} x^{q^{k-1}} \\
&= \alpha(x + \alpha^{q-1} x^q + \alpha^{q^2-1} x^{q^2} + \ldots + \alpha^{q^{k-1}-1} x^{q^{k-1}}) \\
&= \alpha \mathsf{Trace}(x) \ ,
\end{aligned}$$

the last step following as $q^m - 1$ is divisible by $q - 1 \ \forall m \geq 1$ and thus the relevant powers of α reduce to identity. The two properties imply Trace is $\mathbb{F}_q$ linear. □

(c) *Proof.* Viewing F_{q^k} as a vector space over the base prime field, and using the column vector representation for its elements, we must have all linear maps representable as row vectors (/covectors/members of the dual space). Thus, for a linear map L on this vector space, we must be able to represent its action on members of the field as multiplication by the row vector

$$\begin{pmatrix} L_0 & L_2 & \dots & L_{k-1} \end{pmatrix}$$

with its action on some $A \in \mathbb{F}_{q^k}$ given as

$$\begin{pmatrix} L_0 & L_2 & \dots & L_{k-1} \end{pmatrix} \begin{pmatrix} a_0 & a_2 & \dots & a_{k-1} \end{pmatrix}^\top .$$

Consider now a vector B in this space such that for some invertable matrix Λ

$$B = \Lambda^{-1} A$$
$$A = \Lambda B, \text{ with}$$
$$\Lambda = \begin{pmatrix} \lambda_0 & 0 & \dots & 0 \\ \lambda_1 & \lambda_0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \lambda_{k-1} & \lambda_{k-2} & \dots & \lambda_0 \end{pmatrix} .$$

Here, Λ is the multiplicative action of the vector element with coefficients $\{\lambda_i\}$ and its matrix inverse consequently that of the inverse element. (Invertability just requires $\lambda_0 \neq 0$ as this is a triangular matrix. I'm not even sure if this is necessary, and I struggle to resolve it later too.)

We have,

$$LA = L\Lambda B .$$

Our inquiry resolves to whether for any other linear map M, we can find a linear map such that $L\Lambda = M$ and thus $L(\Lambda B) = MB$. Setting L to be Trace reduces to the original problem. Resolving the equations and refactoring with $\{\lambda_i\}$ as the variables in the system, we get

$$\begin{pmatrix} L_0 & 0 & \dots & 0 \\ L_1 & L_0 & \dots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ L_{k-1} & L_{k-2} & \dots & L_0 \end{pmatrix} \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_{k-1} \end{pmatrix} = \begin{pmatrix} M_0 \\ M_1 \\ \vdots \\ M_{k-1} \end{pmatrix}$$

Clearly, this linear system has ≥ 1 solutions. Thus, there always exists a vector element for each linear map (possibly more) such that pre-multiplication by it reduces the linear map to another linear map of choice. Setting choice to Trace gives us the required result. $\square$

Question 2.

(a) To compute for each i,

$$u_i = \frac{1}{\prod_{j \neq i}(\alpha_i - \alpha_j)}$$

divide the denominator into two products of size $\approx \frac{n}{2}$. Combining these is clearly one multiplication, i.e. $\mathcal{O}(1)$. The division itself is a constant order field operation, so I just compute the product first. This has the time complexity recurrence

$$T(n) = 2T(\frac{n}{2}) + \mathcal{O}(1) \ .$$

We obtain the total complexity $\mathcal{O}(\log n)$. Since there are n such quantities to be computed, we get the total complexity to be $\mathcal{O}(n \log n)$.

(b) Suppose we break the problem into instead interpolating two sets of $\frac{n}{2}$ points, with results f_1 and f_2, and writing

$$\begin{aligned} f(x) &= f_1(x)g_1(x) + f_2(x)g_2(x) \\ g_1(x) &= \prod_{i \leq \frac{n}{2}} (x - \alpha_i) \\ g_2(x) &= \prod_{i > \frac{n}{2}} (x - \alpha_i) \end{aligned}$$

The base case is the Lagrange interpolation for a single point.

We can precompute the g polynomials, and knowing them, the larger problem can be computed in $\mathcal{O}\big(n \log^2 n\big)$ since it has the time complexity recurrence relation

$$T(n) = 2T(\frac{n}{2}) + \mathcal{O}(n \log n + n) \ .$$

As for the precomputation, construct the tree with leaves as $(x - \alpha_i)$ and the layers above them constructed as the products of pairs of the elements of the previous layer. Clearly, these are exactly the g polynomials required. The time recurrence relation again, with the combination step being the multiplication of two $\frac{n}{2}$ degree polynomials, is

$$T(n) = 2T(\frac{n}{2}) + \mathcal{O}(n \log n) \ .$$

Total time complexity is thus their sum $\mathcal{O}\big(n \log^2 n\big) = \mathcal{O}(n \mathsf{poly} \log n)$.

Question 3.

Since the question asks to pick points for arbitrarily large n, it is assumed here that the field itself is sufficiently large to allow picking points arbitrarily.

Consider for any set of t distinct points in $\mathbb{F}^2$, their evaluation over a polynomial in $\mathbb{F}[x, y]$ with degree $n \geq 2$,

$$\forall i \in \{0, 1, \ldots, t\}\ P(\alpha_i, \beta_i) = \sum_{j+k<n;j,k\geq 0} a_{jk}\alpha_i^j \beta_i^k \ .$$

We can write this as the (generally) non-homogeneous linear system

$$\begin{pmatrix} \alpha_1^0\beta_1^0 & \alpha_1^0\beta_1^1 & \ldots & \alpha_1^0\beta_1^n & \alpha_1^1\beta_1^0 & \ldots & \alpha_1^n\beta_1^0 \\ \alpha_2^0\beta_2^0 & \alpha_2^0\beta_2^1 & \ldots & \alpha_2^0\beta_2^n & \alpha_2^1\beta_2^0 & \ldots & \alpha_2^n\beta_2^0 \\ & & & \vdots & & & \\ \alpha_t^0\beta_t^0 & \alpha_t^0\beta_t^1 & \ldots & \alpha_t^0\beta_t^n & \alpha_t^1\beta_t^0 & \ldots & \alpha_t^n\beta_t^0 \end{pmatrix}_{t\times\binom{n+2}{2}} \begin{pmatrix} a_{00} \\ a_{01} \\ \vdots \\ a_{n0} \end{pmatrix}_{\binom{n+2}{2}\times 1} = \begin{pmatrix} P(\alpha_1, \beta_1) \\ P(\alpha_2, \beta_2) \\ \vdots \\ P(\alpha_t, \beta_t) \end{pmatrix}_{t\times 1} .$$

Conversely, we can replace $P(\alpha_i, \beta_i)$ by λ_i and look for the parameters a_{jk} which describe the interpolating polynomial. Our problem reduces to showing that there exists a pair of a $t \times n^2$ matrix and a t-vector such that the system has no solutions, i.e. no interpolating polynomial exists, for sufficiently bounded t ($\leq \binom{n+2}{2}$ as given).

Consider $\beta_i = 0\ \forall i$. This is a univariate interpolation with the linear system

$$\sum_{j=0}^{n} a_{j0}\alpha_i^j, i \in \{1, 2, \ldots, t\} \ .$$

Choose t such that $n + 1 < t \leq \binom{n+2}{2}$. This is clearly a (possibly highly) overdetermined system. We can construct a set of input points that have no solution as follows: pick the first $n + 1$ points arbitrarily. These produce a unique solution for the coefficients $P\{a_{j0}\}$. Construct the next $(t-n-1)$ points such that they explicitly violate the constructed (univariate) polynomial, i.e., $\lambda_j \neq P(\alpha_j, 0)$ for atleast one $j \in \{n+2, \ldots, t\}$. Obviously, this system has no solution. This produces the required set of points.