

The Finite Fast Fourier Transform

Kirill Levchenko

Let n be a power of two, and let \vec{u} and \vec{v} be two vectors in $\text{GF}(q)^n$, where $q = an + 1$ for some integer $a > 1$, and $\text{GF}(q)$ has characteristic greater than n . Define $\vec{w} \in \text{GF}(q)^n$ as

$$w_k = \sum_{\substack{i+j \equiv k \\ (\text{mod } n)}} u_i v_j.$$

It is easy to see that we can compute \vec{w} in quadratic time: what is remarkable is that it can be done in $O(n \log n)$ time using the Fast Fourier Transform, which we describe shortly. We will need an algebraic fact first.

Let β be a non-zero element of order m in $\text{GF}(q)$, where $1 < m < n$. Note that $2|m$, and furthermore,

Lemma 1. $\beta^{m/2} = -1$.

Proof. Note that $(\beta^{m/2})^2 = \beta^m = 1$, so

$$\begin{aligned} 0 &= (\beta^{m/2})^2 - 1 \\ &= (\beta^{m/2})^2 - 1^2 \\ &= (\beta^{m/2} + 1)(\beta^{m/2} - 1). \end{aligned}$$

From $\beta^{m/2} \neq 1$, it follows that $\beta^{m/2} = -1$. □

Let $\alpha \in \text{GF}(q)$ have order n , and consider the vectors $\vec{x}, \vec{y} \in \text{GF}(q)^n$ defined as follows.

$$x_\ell = \sum_i u_i \alpha^{i\ell} \quad \text{and} \quad y_\ell = \sum_i v_i \alpha^{i\ell}.$$

Now let $z_\ell = x_\ell y_\ell$, equivalently

$$z_\ell = \sum_{i,j} u_i v_j \alpha^{(i+j)\ell}.$$

Now consider

$$\sum_\ell z_\ell \alpha^{-k\ell}$$

for some k . We can re-arrange the summation to obtain

$$\begin{aligned} \sum_\ell z_\ell \alpha^{-k\ell} &= \sum_\ell \sum_{i,j} u_i v_j \alpha^{(i+j-k)\ell} \\ &= \sum_{i,j} \sum_\ell u_i v_j \alpha^{(i+j-k)\ell} \\ &= \sum_{i,j} u_i v_j \sum_\ell \alpha^{(i+j-k)\ell}. \end{aligned}$$

If $i + j \equiv k \pmod{n}$ then $\alpha^{(i+j-k)} = 1$. Otherwise, let $\beta = \alpha^{(i+j-k)} \neq 1$ and let $m > 1$ be the order of β . Note that $m|n$. We now write the sum as

$$\begin{aligned}
\sum_{i,j} u_i v_j \sum_{\ell} \alpha^{(i+j-k)\ell} &= \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j \sum_{\ell} 1 + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \sum_{\ell} \beta^{\ell} \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \cdot \frac{n}{m} \sum_{\ell=0}^{m-1} \beta^{\ell} \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \cdot \frac{n}{m} \left(\sum_{\ell=0}^{m/2-1} \beta^{\ell} + \sum_{\ell=0}^{m/2-1} \beta^{m/2+\ell} \right) \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \cdot \frac{n}{m} \left(\sum_{\ell=0}^{m/2-1} \beta^{\ell} + \sum_{\ell=0}^{m/2-1} \beta^{m/2+\ell} \right) \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \cdot \frac{n}{m} \left(\sum_{\ell=0}^{m/2-1} \beta^{\ell} - \sum_{\ell=0}^{m/2-1} \beta^{\ell} \right) \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j + \sum_{\substack{i+j \not\equiv k \\ \pmod{n}}} u_i v_j \cdot \frac{n}{m} \cdot 0 \\
&= n \sum_{\substack{i+j \equiv k \\ \pmod{n}}} u_i v_j
\end{aligned}$$

The field $\text{GF}(q)$ has characteristic greater than n , so $n \cdot 1 \neq 0$. Writing n^{-1} for $(\sum_{i=0}^{n-1} 1)^{-1}$, we have

$$w_k = n^{-1} \sum_{\ell} x_{\ell} y_{\ell} \alpha^{-k\ell}.$$

On the surface of it, the above still requires quadratic time. However we can do better by observing that

$$x_{\ell} = \sum_{i=0}^{n-1} u_i \alpha^{i\ell} = \sum_{i=0}^{n/2-1} u_{2i} \alpha^{2i\ell} + \alpha^{\ell} \sum_{i=0}^{n/2-1} u_{2i+1} \alpha^{2i\ell}$$

and

$$\begin{aligned}
x_{n/2+\ell} &= \sum_{i=0}^{n-1} u_i \alpha^{i(n/2+\ell)} = \sum_{i=0}^{n/2-1} u_{2i} \alpha^{2i(n/2+\ell)} + \alpha^{n/2+\ell} \sum_{i=0}^{n/2-1} u_{2i+1} \alpha^{2i(n/2+\ell)} \\
&= \sum_{i=0}^{n/2-1} u_{2i} \alpha^{in} \alpha^{2i\ell} + \alpha^{n/2} \alpha^{\ell} \sum_{i=0}^{n/2-1} u_{2i+1} \alpha^{in} \alpha^{2i\ell} \\
&= \sum_{i=0}^{n/2-1} u_{2i} \alpha^{2i\ell} - \alpha^{\ell} \sum_{i=0}^{n/2-1} u_{2i+1} \alpha^{2i\ell}.
\end{aligned}$$

Define $f(\vec{u}, n, \alpha)$ to return the vector $\vec{\phi}$ whose ℓ^{th} entry is

$$\sum_{i=0}^{n-1} u_i \alpha^{i\ell}.$$

Let \vec{u}^e be the even-indexed entries of \vec{u} and let \vec{u}^o be the odd-indexed entries of \vec{u} . Then $f(\vec{u}, n, \alpha)$ can be computed by first computing $\vec{\phi}^e = f(\vec{u}^e, n/2, \alpha^2)$ and $\vec{\phi}^o = f(\vec{u}^o, n/2, \alpha^2)$. Then the ℓ^{th} entry of $f(\vec{u}, n, \alpha)$ is

$$\phi_\ell = \begin{cases} \phi_\ell^e + \alpha^\ell \phi_\ell^o & \ell < n/2 \\ \phi_\ell^e - \alpha^\ell \phi_\ell^o & \ell \geq n/2. \end{cases}$$

This gives running time $O(n \log n)$ as desired.