.I Factorization Algorithms

.I.1 Berlekamp's Algorithm.

The following algorithm, due to Berlekamp, for factorization of polynomials works over small fields, where the size of the field is to be measured against the degree of the polynomial to be factored.

It is based on a striking application of the C.R.T.

Our ground field is the field k with $q = p^n$ elements, e.g., $q = 2$. Let $f(X) \in k[X]$ denote the polynomial under consideration. We may assume that $f(X)$ has no multiple factors. This is easy to check, by an application of Euclid to f and its formal derivative $f'(X)$. So assume $f(X) = f_1(X) \cdot \ldots \cdot f_k(X)$ where the f_j are irreducible monic over k, no two equal, hence relatively prime in pairs.

Solve, for any $c_j \in k$ the simultaneous congruences

$$h(X) \equiv c_j \pmod{f_j} \;\; j = 1, 2, \ldots k$$

and choose a solution of degree $< n$, the degree of f.

Since the c_j belong to k we have $c_j^q = c_j$, so the congruences above are satisfied by $h(X)^q = h(X^q)$, too. (Freshman's dream, note that the coefficients a_i of $h(X)$ satisfy $a_i^q = a_i$.)

So we have

$$h(X^q) = h(X)^q \equiv h(X) \pmod{f(X)}$$

by the uniqueness part of the C.R.T.

On the other hand, from the factorization

$$X^q - X = \prod_{c \in k} (X - c)$$

we get

$$h(X)^q - h(X) = \prod_{c \in k} (h(X) - c)$$

If the left member is divisible by $f(X)$ each f_j must be a factor of one of the $h(X) - c$ so $h(X)$ must satisfy some system of congruences of the form $h(X) \equiv c_j \pmod{f_j}$ above.

So there is a bijection between solutions (modulo $f(X)$) of C.R.T. congruences of the above type and solutions to $h(X)^q - h(X) \equiv 0 \pmod{f(X)}$

Now the mapping

$$F(h(X)) = h(X^q) \pmod{f(X)}$$

of the k-vector space $V = k[X]/(f(X))$ is obviously linear. The $h(X)$ answering our needs are those for which

$$F(h(X)) \equiv h(X) \pmod{f(X)}$$

i.e., the eigenvectors to the eigenvalue 1. If the dimension of the eigenspace is d, then there are q^d solutions. On the other hand, the system of congruences has q^k solutions. By the bijection noted above, we see that $d = k$! In particular, if the dimension is 1 (i.e., if all solutions are constants), $f(X)$ is irreducible.

It could very well happen that several irreducible factors divide the same $h(X) - c$ (cf. example below), where $h(X)$ is some basis element of the eigenspace. However, for any pair f_i, f_j there is at least one $h(X)$ and a constant c such that f_i, but not f_j, divides $h(X) - c$. This follows easily from the fact that the C.R.T congruneces above are solvable for all choices of right members c_j, exercise.

Let us give an easy (too easy) example.

.I.2 Example: Let $k = \mathbf{Z}_2$ anf $f(X) = X^7 - 1$. Since $X^{2^3} - X$ is the product of all monic irreducible polynomials of degrees 1 and 3 we expect to find the obvious factor $X - 1 (= X + 1)$ along with two irreducible polynomials of degree 3.

Modulo $X^7 - 1$ we have

$$F\begin{pmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{pmatrix} = \begin{pmatrix} 1 & x^2 & x^4 & x^6 & x & x^3 & x^5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & x & x^2 & x^3 & x^3 & x^4 & x^5 & x^6 \end{pmatrix} B$$

Subtracting (i.e.,adding) 1 from the diagonal, and solving the homogenous system $(B + I)X = 0$ (do!) we see that all solutions are linear combinations of $1, X^4 + X^2 + X, X^6 + X^5 + X^3$.

Let us try $h_1(X) = X^4 + X^2 + X$ first. By Euclid, or mere inspection, we find $(f(X), h_1(X)) = X^3 + X + 1 = f_1(X)$, which is irreducible. Dividing $f(X)$ by this factor we get $g_1(X) = X^4 + X^2 + X + 1$. Trying $h_1(X) + 1 = X^4 + X^2 + X + 1$ leads us nowhere so next we try $h_2(X) = X^6 + X^5 + X^3 = X^3(X^3 + X^2 + 1)$ so we get the factor $f_2(X) = X^3 + X^2 + 1$ right away. Dividing $g_1(X)$ by $f_2(X)$ gives us the remaining factor $X + 1$.

So we need not look any further. The reader may wish to check that the factors $X + 1$ and $X^3 + X + 1$ do divide $h_2(X) + 1$ as predicted by the theory. ∎

If F has multiple factors $f_i^{e_i}$, then replacing the f_i by these powers in the C.R.T congruences, we may easily modifiy our reasoning to prove that the eigenspace dimension considered still equals the number of distinct irreducible factors in f. The algorithm will produce these powers.

.I.3 $X^n - 1$**,** *Method of idempotents.*

Let us return to cyclic codes. We wish to study the factorization of $F(X) = X^n - 1 = X^n + 1$, n odd, over $k = \mathbf{Z}/(2)$.

Assume that $F(X) = f_1(X) \cdot \ldots \cdot f_d(X)$ where the f_i are irreducible, monic, no two equal. Recall that

$$R = k[X]/(f(X)) \simeq \oplus k[X]/(f_i(X)) = \oplus F_i = \oplus Re_i$$

where the F_i are fields and the e_i are a complete set of orthogonal idempotents, $e_i e_j = \delta_{ij}$, $1 = \sum_i e_i$.

By the proof of the C.R.T each e_i is divisible by all the $f_j, j \neq i$. e_i differs from the product $f(X)/f_i(X)$ by a factor that is relatively prime to $f(X)$. By the same token $1 - e_i = 1 + e_i = \sum_{j \neq i} e_j$ is f_i times some factor that is relatively prime to f. So knowing the idempotents we can easily find the $f_i = (1 + e_i, f)$ by Euclid. Actually, the idempotents might be more interesting in many cases.

Since $Re_i = F_i$ is a field, possessing no proper ideals except (0) it is minimal ideal of R. We call e_i a *primitive idempotent.*

In 17.III.1. we saw that any ideal of R is generated by an idempotent, which is a sum of some of the e_i. The idempotents form a vector space over k, of dimension d, since the e_i obviously span this space and equally obviously are linearly independent.

If we partition the e_i into disjoint subsets, and sum within each set we obtain idempotents that are still mutually orthogonal. If two sets of primitive idempotents have at least one element, e_j, in common then the sums of each set will not be mutually ortohogonal since e_j will survive the multiplication.

So, in any set of mutually orthogonal idempotents g_i, each element is the sum of e_i:s and the sets making up the various g_i are mutually disjoint. From this we see that the only basis (of the space of idempotents) consisting of orthogonal idempotents is the one consisting of the primitive idempotents e_i.

To be explicit we now let $n = 15 = 2^4 - 1$. The general theory of finite fields tells us what to expect. The polynomial $X^{16} - X$ is the product of all monic irreducible polynomials of degrees 1,2,4 so $X^{15} - 1$ has one factor $X + 1$ of degree 1, one factor of degree 2 (viz., $X^2 + X + 1$) along with three factors of degree 4, five factors in all.

It is easy to find *one* basis for the space of idempotents. By Freshman's Dream,

$$(\ldots + X^k + \ldots)^2 = (\ldots + X^{2k} + \ldots)$$

where the exponents are to be taken modulo 15. I.e., if an idempotent contains the term X^k it must contain X^{2k} (exponent modulo 15). From this we see immediately

that every idempotent is a linear combination of

$$g_1(X) = 1;\ \ g_2(X) = X + X^2 + X^4 + X^8;$$

$$g_3(X) = X^3 + X^6 + X^{12} + X^9;\ \ g_4(X) = X^5 + X^{10};$$

$$g_5(X) = X^7 + X^{14} + X^{13} + X^{11}$$

For the construction of each g_i I simply picked one exponent and kept doubling it until I got a repeat.

The g_i span the space of idempotents by the discussion above. Since no two of them have any X-power in common they are linearly independent, so we have found a basis (and we see again that the number of irreducible factors is 5).

The identity

$$1 = (1 + g_2(X)) + g_2(X) = h_1(X) + h_2(X)$$

is a decomposition of 1 into to orthogonal idempotents. We wish to decompose them further.

Now if g is an idempotent satisfying $gh_i = 0$ or $(1 + g)h_i = 0, i = 1, 2$, (so that $gh_i = h_i$ in the latter case) then

$$g = gh_1 + gh_2 = h_1 \text{ or } h_2$$

so for some g_i we must have $g_i h_1 \neq 0, (1 + g_i)h_2 \neq 0$ and

$$1 = g_i h_1 + (1 + g_i)h_1 + h_2$$

is a decomposition of 1 into three ortohogonal idempotents.

It turns out that

$$g_3(1 + g_2) = g_2 + g_3 \neq 0;\ \ (g_3 + 1)(g_2 + 1) = g_3 + 1 \neq 0$$

(check this) so we get

$$1 = g_2 + (g_2 + g_3) + (1 + g_3)$$

and the three terms are mutually orthogonal.

Again, for some g_j, and one of these three terms, we must have that neither g_j nor $g_j + 1$ kills it; otherwise, by the same reasoning as above, all g_j would be linear combinations of the three idempotents. Testing g_4 against g_2 we get the orthogonal sum $g_2 = (g_3 + g_5) + (g_2 + g_3 + g_5)$. Finally, testing g_4 against $1 + g_3$, we get the primitive idempotents

$$e_1 = g_3 + g_5;\ \ e_2 = g_2 + g_3 + g_5;\ \ e_3 = g_2 + g_3;$$

$$e_4 = g_2 + g_4 + g_5 \quad e_5 = g_1 + g_2 + g_3 + g_4 + g_5$$

Here, for instance,

$$e_1 = X^3 + X^6 + X^7 + X^9 + X^{11} + X^{12} + X^{13} + X^{14}$$

and,

$$f_1 = (f, 1 + e_1) = X^4 + X^3 + 1$$

The remaining factors are

$$f_2 = X^4 + X^3 + X^2 + X + 1$$

(note that $f_2(X)(X + 1) = X^5 + 1$ so this factor takes care of the roots of order 5),

$$f_3(X) = X^4 + X + 1$$

(the reciprocal of f_1, i.e., the one gotten by inverting the roots).

$$f_4(X) = X^2 + X + 1$$

(taking care of roots of order 3) and,

$$f_5(X) = X + 1$$

(obvious).