MAT 148, Winter 2016
Solutions to HW 6

D. (50 points) Consider a field F with 2^n elements. It is known that $1+1=0$ in F.

a) Prove that if $a^2=b^2$ then $a=b$ $(a,b\in F)$.

Solution: Since $a^2-b^2=(a-b)(a+b)=0$, either $a-b=0$ or $a+b=0$. Since $1=(-1)$ in F, $a=b$.

b) Prove that the function $\Phi(x)=x^2$ is a bijection from F to itself.

Solution: By (a) Φ is injective (sends different elements to different elements), therefore the image of Φ contains 2^n different elements, so Φ is surjective (every element is in the image) and therefore bijective.

c) Prove that every element in F has a unique square root.

Solution: Since Φ is a bijection, it has a well-defined inverse map, so for every y there is a unique element x such that $x^2=y \Leftrightarrow x=\sqrt{y}$.

d) Prove that $\Phi(x+y)=\Phi(x)+\Phi(y)$ and $\Phi(xy)=\Phi(x)\Phi(y)$ for all $x,y\in F$.

Solution: $\Phi(x+y)=(x+y)^2=x^2+y^2 \mod 2, \Phi(xy)=(xy)^2=x^2y^2$.

e) Describe Φ explicitly for $F=GF(16)$.

Solution: We know that every nonzero element of $GF(16)$ is a power of x and $x^{15}=1$, therefore:

$$\Phi(0)=0,\ \Phi(1)=1,\ \Phi(x)=x^2,\ \Phi(x^2)=x^4,\ \Phi(x^3)=x^6,\ \Phi(x^4)=x^8,\ \Phi(x^5)=x^{10},$$
$$\Phi(x^6)=x^{12},\ \Phi(x^7)=x^{14},\ \Phi(x^8)=x^{16}=x,\ \Phi(x^9)=x^3,\ \Phi(x^{10})=x^5,$$
$$\Phi(x^{11})=x^7,\ \Phi(x^{12})=x^9,\ \Phi(x^{13})=x^{11},\ \Phi(x^{14})=x^{13}.$$

12. (25 points) Perform the following computations in $GF(16)$ (field with 16 elements).

a) $1001\cdot 1011+0101/1100$;

Solution: Let $f(x)=x^4+x^3+1$, then $GF(16)=\mathbb{Z}_2[x]/(f(x))$. $1001=x^3+1, 1011=x^3+x+1$, so

$$1001\cdot 1011=(x^3+1)(x^3+x+1)=x^6+x^4+x^3+x^3+x+1=x^6+x^4+x+1=$$

$$x^2(x^4+x^3+1)+x^5+x^4+x^2+x+1=$$
$$x^2(x^4+x^3+1)+x(x^4+x^3+1)+x^2+1=x^2+1 \mod f(x).$$

Furthermore, $0101 = x^2+1$, $1100 = x^3+x^2$. Since $x(x^3+x^2)+1 = f(x)$ then $1/1100 = x$, so

$$0101/1100 = (x^2+1)/(x^3+x^2) = (x^2+1)x = x^3+x.$$

Finally,

$$1001 \cdot 1011 + 0101/1100 = x^3+x^2+x+1.$$

b) $\sqrt{1110} + 1101$;

Solution: $1110 = x^3+x^2+x = x^8$, so $\sqrt{1110} = x^4 = x^3+1$. Therefore

$$\sqrt{1110}+1101 = x^3+1+x^3+x^2+1 = x^2.$$

c) $\sqrt{1000}$.

Solution: $1000 = x^3$, so $\sqrt{x^3} = \sqrt{x^{18}} = x^9 = x^2+1$.

15a. (25 points) Using the double-error-correcting BCH code, decode the vectors

a)$(0,1,0,0,0,0,0,1,0,0,0,0,0,0,0)$

Solution: Since the zero vector is a codeword for any linear code, this vector is different from it in two bits, and the code corrects two errors, the original message was $(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$.

b)$(1,1,1,0,1,1,1,1,1,1,1,1,1,1,1)$

Solution: Similarly, one can check using the parity check matrix that the vector $(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)$ is a codeword, and this vector differs from it in one bit. Therefore the original message was $(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)$.