Finite Field Embeddings

Christopher Smith

Last Updated: July 1, 2025

1 Motivation

Recently, I have found myself working a lot with the MP-SPDZ engine for secure multi-party computation (MPC). In particular, I have been interested in understanding how a certain MPC script implementing AES works: `https://github.com/data61/MP-SPDZ/blob/master/Programs/Source/aes.mpc`. I naively expected the script to be a straightforward translation of the official FIPS 197 standard for AES, and was quite confused when I kept running into code referencing some kind of "embedding" in nearly every part of the implementation. As it turns out, the "embedding" in question was referring to *field embeddings*, that is, *ring homomorphisms* between fields. No such embedding is ever referenced in FIPS 197, so why does it appear here?

I found my answer in the following GitHub issue: `https://github.com/data61/MP-SPDZ/issues/8`. In the high-level Python interface exposed by MP-SPDZ for describing MPC circuits, developers are given access to data types `sgf2n` and `cgf2n` for operating on elements in the finite field $GF(2^n)$. This is great, since AES frequently uses the field on 256 elements $GF(2^8)$. Unfortunately, according to the above GitHub issue, the security of MPC protocols implemented in MP-SPDZ depends on a large field, and $GF(2^8)$ is simply too small for maliciously secure protocols. It is for this reason that the AES script linked above assumes that the MPC protocols be configured for $GF(2^{40})$, and uses an embedding of $GF(2^8)$ into $GF(2^{40})$. This way, when we need to perform arithmetic over elements $GF(2^8)$, we can first map them into $GF(2^{40})$, perform the arithmetic in this larger field using the `sgf2n`/`cgf2n` types, and translate the result back to $GF(2^8)$ with the (left) inverse of the embedding.

Because I found these embeddings to be fascinating in their own right, in what follows I take a stab at exploring what embeddings are, when they exist, how to compute their descriptions, and how to evaluate them. I am hoping a reader with a basic understanding of algebraic concepts like groups, rings, fields, homomorphisms and their kernels, ideals, and quotient spaces finds this to be a smooth read. I try to make sure anything I do not explicitly define is easily found on Wikipedia.

2 Defining Embeddings

As one may have deduced by now, an embedding - broadly speaking - is an injective structure-preserving map between two mathematical structures [Wik25]. In an algebraic context, "structure-preserving" maps are homomorphisms, so it makes sense to try and define a field embedding as an injective field homomorphism. While there is nothing technically wrong with this definition, it is a bit redundant. A field homomorphism is simply a ring homomorphism between fields, and ring homomorphisms between fields are always injective, so **a field embedding is typically just defined**

as a ring homomorphism between fields. Because the injectivity of field homomorphisms was not immediately obvious to me, let us take a moment to establish this fact.

Claim 1 (Field homomorphisms are injective [Wik25])**.** *If $\phi : E \to F$ is a ring homomorphism between fields (*i.e.*, a field homomorphism, or a field embedding), then ϕ is injective.*

Proof. If ϕ were not injective, then $\exists x \neq y \in E : \phi(x) = \phi(y)$, so $\phi(x) - \phi(y) = \phi(x - y) = 0 \implies (x - y) \in \ker(\phi) \neq \{0_E\}$. Thus, it suffices to show that ϕ is injective by showing that its kernel is the zero ideal. Recall that the kernel of any ring homomorphism is an ideal ($0_E \in \ker(\phi)$; $\phi(x + y) = 0_F \ \forall x, y \in \ker(\phi)$; $\phi(-x) = \phi(-1) \cdot \phi(x) = 0 \ \forall x \in \ker(\phi)$; and $\forall a \in E, \forall x \in \ker(\phi) : \phi(ax) = \phi(a) \cdot \phi(x) = 0$). Further observe that an ideal of a field must either be the zero ideal, or the field itself. This is because if there exists a non-zero element x in the ideal of a field, then $x^{-1}x = 1$ is also in this ideal, and it follows that every element of the field must belong to this ideal. But clearly $\ker(\phi) \neq F$, since $\phi(1_E) = 1_F \neq 0_F$. Thus, $\ker(\phi) = \{0_E\}$. □

The connotation of the word "embedding" seems to imply that the smaller field "lives inside" the larger field, in some sense. The following claim captures this sentiment precisely.

Claim 2 (Image of field embedding is a subfield)**.** *Let $\phi : E \to F$ be a field embedding. Then the image of ϕ, denoted* $\mathrm{Im}(\phi)$*, is a subfield of F.*

Proof. Because ϕ is a ring homomorphism, we already know $\mathrm{Im}(\phi)$ is a subring of F, so it remains to show that every non-zero element in $\mathrm{Im}(\phi)$ has a multiplicative inverse. Let $y \in \mathrm{Im}(\phi)$ be non-zero. Then $y = \phi(x)$ for some non-zero $x \in E$. See that $\phi(x^{-1}) \cdot \phi(x) = \phi(x^{-1} \cdot x) = \phi(1_E) = 1_F$, so $y^{-1} = \phi(x^{-1}) \in \mathrm{Im}(\phi)$. □

3 Existence of Field Embeddings

A natural question to ask is whether given two fields E and F, an embedding $E \hookrightarrow F$ exists. From here on we will only concern ourselves with the case of finite fields. We present a few helper lemmas before the main result of Theorem 5.

Lemma 3 (Characteristic of codomain divides characteristic of domain for a ring homomorphism)**.** *Let $\phi : R \to S$ be a ring homomorphism. Then the characteristic of S divides the characteristic of R.*

Proof. Let $n = \mathrm{char}(R)$ and $m = \mathrm{char}(S)$. Viewing R and S as additive groups, $n = \mathrm{ord}(1_R)$ and $m = \mathrm{ord}(1_S)$. Observe that $0_S = \phi(0_R) = \phi(n \cdot 1_R) = n \cdot 1_S$. Now assume for contradiction that $m \nmid n$. By Euclidean division, we have $n = mq + r$ for unique integers q, r, where $0 < r < m$. Then we have that $n \cdot 1_S = (mq + r) \cdot 1_S = r \cdot 1_S$. But $r \cdot 1_S \neq 0_S$, since $r < m$ and $m = \mathrm{ord}(1_S)$ is by definition the smallest such integer with this property. Thus, $m|n$. □

Lemma 4 (Subfield exists iff extension degrees divide)**.** *A field of order p^r contains a field of order p^k if and only if $k|r$.*

Proof. See the proof of Theorem 15.7.3(e) in [Art11]. □

Theorem 5 (Existence of (Finite) Field Embeddings)**.** *Let E and F be finite fields. There exists an embedding $\phi : E \to F$ if and only if E and F have the same characteristic, and the extension degree of E divides the extension degree of F.*

Proof. Suppose $\phi : E \to F$ is a field embedding. Because ϕ is a ring homomorphism, by Lemma 3, $\operatorname{char}(F) | \operatorname{char}(E)$. But E and F are finite fields, so their characteristics are prime, and so it must be the case that $\operatorname{char}(E) = \operatorname{char}(F) = p$ for some prime p. Furthermore, we now have that $\operatorname{ord}(E) = p^k$ and $\operatorname{ord}(F) = p^r$ for some positive integers k, r. By Claim 2, we know that $\operatorname{Im}(\phi)$ is a subfield, and the injectivity of ϕ tells us that the size of this subfield is p^k. Thus, by Lemma 4, we have $k|r$.

In the other direction, we know $\operatorname{char}(E) = \operatorname{char}(F) = p$ for some prime p, and we know $k|r$, so by Lemma 4, F contains a subfield E' of order p^k. It is a well-known fact that fields of the same size are isomorphic, so there exists an isomorphism $\phi : E \to E'$. But since $E' \subseteq F$, we can instead view ϕ as a ring homomorphism from E to F with image E'. In other words, ϕ is an embedding of E into F. □

4 Computing Descriptions of Field Embeddings

Applying Theorem 5 to the case of $GF(2^8)$ and $GF(2^{40})$, we can see that there must exist an embedding of the former into the latter. But can we succinctly describe this embedding. And even if the embedding has a succinct description, can we compute the description efficiently. The answer to the first question is yes: embeddings can be described essentially by a pair of elements - one in the smaller field and one in the larger field. The answer to the second question is also yes, but due to the variety of approaches and the technical detail involved [BFD+17], we settle for instructions on how to use a computer algebra system like SageMath for computing these descriptions. Note that, according to [BFD+17], computing embeddings is a natural task for computer algebra systems.

4.1 Describing Field Embeddings

Suppose $\phi : E \to F$ is a field embedding. By Theorem 5, we know there exists a prime p, and positive integers k, r such that $\operatorname{ord}(E) = p^k$, $\operatorname{ord}(F) = p^r$ (and $k|r$). Since fields are uniquely characterized by their order up to isomorphism, we can give E and F explicit descriptions via the canonical construction of extension fields as quotient rings. Specifically, let $\mathbb{Z}_p[x]$ be the polynomial ring with coefficients in $\mathbb{Z}_p$ (a prime field), and let $f(x) \in \mathbb{Z}_p[x]$ be a degree k irreducible polynomial. Then E is isomorphic to the quotient ring $\mathbb{Z}_p[x]/(f(x))$. Similarly, F is isomorphic to $\mathbb{Z}_p[y]/(g(y))$ for $g(y) \in \mathbb{Z}_p[y]$ a degree r irreducible polynomial.

With these field descriptions, we can now view ϕ as a function sending some element of E, which we can represent as a polynomial $\sum_{i=0}^{k-1} a_i x^i$ with $a_i \in \mathbb{Z}_p$, to an element of F, which we can represent as another polynomial $\sum_{i=0}^{r-1} b_i y^i$ with $b_i \in \mathbb{Z}_p$. At this point, we technically have enough information to describe ϕ by its function table, but obviously this description is potentially huge: p^{k-1} rows with $r - 1 \cdot \log(p)$ bits in each entry. To obtain a succinct description we need additional insight into the structure of ϕ.

The key insight is that E and F are both vector spaces over the same base field $\mathbb{Z}_p$, so ϕ is a homomorphism between vector spaces, *i.e.*, a linear transformation. This means if we pick a basis E, in order to describe ϕ it suffices to list the image of the basis under ϕ. Because E is a k-dimensional vector space, it appears we only need $k \cdot (r-1) \cdot \log(p)$ bits to describe ϕ. Actually, we can do even better. Let us pick the so-called "primitive element" basis $\{1, x, x^2, ..., x^{k-1}\}$ of E, and

$\{1, y, y^2, ..., y^{r-1}\}$ for F. As a quick aside, notice we already implicitly assumed these bases in the previous paragraph when we stated elements of E and F could be represented as polynomials in x and y. We have also abused notation slightly in that we have also been using x as the free variable in the polynomial ring $\mathbb{Z}_p[x]$, but the x appearing in the primitive element basis is technically different as it is a root of $f(x)$, and so it is usually renamed to something like α. These are unnecessary details for our purposes, since the point is that we can represent elements of E as polynomials in some variable x, and hence the set $\{1, x, x^2, ..., x^{k-1}\}$ constitutes a basis for E. Of course, the same goes for y, g, and F. Back to the task at hand, how should ϕ map each element of this basis? Clearly we must have $\phi(1) = 1$ since ϕ is a ring homomorphism. Now suppose $\phi(x) = z$ for some $z \in F$. Then $\phi(x^2) = z^2, \phi(x^3) = z^3, ..., \phi(x^{k-1}) = z^{k-1}$. In other words, ϕ **is completely described by where we choose to send** x. This is indeed a succinct description, as it requires only $(r-1) \cdot \log(p)$ bits.

As a concrete example, the embedding of $GF(2^8)$ into $GF(2^{40})$ used by MP-SPDZ is given by $x = y^5+1$, where $GF(2^8) = \mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$, and $GF(2^{40}) = \mathbb{Z}_2[y]/(y^{40}+y^{20}+y^{15}+y^{10}+1)$.

4.2 Computing Descriptions

Now that we know a field embedding $\phi : E \to F$ can be described solely by where it sends the primitive element $x \in E$, it remains to be seen how to compute this description for a given E and F. That is, how can we find $z \in F$ such that $\phi(x) = z$ describes a valid field embedding? To provide some intuition, notice that x is a root of the polynomial modulus f for E, so in order for ϕ to "preserve structure", z should also be a root of f. More precisely, x and z should share the same *minimal polynomial*. Clearly, we could find such a root z with a brute force approach, but this would take exponential time.

As previously mentioned, we sidestep the details on how to compute this description more efficiently and instead provide an example with SageMath (which if you have never used Sage before it is a wonderful tool: a free open source wrapper over various fast numerical computing libraries, and the language itself is literally just Python with a small handful of syntactic sugar additions to make your life easier).

```
# set up fields
E.<a> = GF(2^8, name='a', modulus=x^8 + x^4 + x^3 + x + 1)
F.<b> = GF(2^40, name='b', modulus=x^40 + x^20 + x^15 + x^10 + 1)

# an_embedding() computes one embedding. embeddings() computes all embeddings.
f = E.an_embedding(F)
assert(f(a) == b^5 + 1)

# to go back and forth between fields, we need the left inverse of f.
g = f.section()
el = F.random_element()
assert(g(f(a)) == a)
```

Listing 1: Embedding $GF(2^8) \hookrightarrow GF(2^{40})$ in Sage

References

[Art11] M. Artin. *Algebra.* Pearson Prentice Hall, 2011.

[BFD$^+$17] Ludovic Brieulle, Luca De Feo, Javad Doliskani, Jean-Pierre Flori, and Éric Schost. Computing isomorphisms and embeddings of finite fields. *CoRR*, abs/1705.01221, 2017.

[Wik25] Wikipedia contributors. Embedding — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Embedding&oldid=1281481383`, 2025. [Online; accessed 15-June-2025].